DEPARTMENT OF
MATHEMATICS

MACQUARIE
University

DMTH137 S2 2017

Discrete Mathematics I

Tutorial Week 13

NAME: Some Student

Student Id: 00000000

Tutorial Group: Z1, Mon 23:00, Z9A 111

Tutor: A Tutor

There is no more 'Homework' to hand in, so ignore the mark box below.

FEEDBACK		
Work	Presentation	Total

DMTH137 Discrete Mathematics I, S2 2017, Tutorial Week 13

1 Tutorial questions for you

This section contains the problems you should attempt at home in preparation for your tutorial.

1. For each $a \in \{0, 1, 2, \ldots, 20\}$, compute $a^5 \bmod 21$.
   (HINT: after having done $1, 2, \ldots, 10$ there is an easy way to get the rest. What is it?)

2. Use your results from the previous question to compute $a^{25} \bmod 21$ for each $a \in \{0, 1, 2, \ldots 20\}$.
   Do you find this result surprising?

3. For the following table of a Boolean function of x, y and z, write down a formula for $F(x, y, z)$ in *disjunctive normal form* (i.e., a sum of products), and also a formula in *conjunctive normal form* (a product of sums).

x	y	z	$F(x, y, z)$
1	1	1	0
1	1	0	1
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	0
0	0	1	1
0	0	0	1

4. Suppose we have the Boolean variables x, y, z and w.
   How many distinct minterms are there using these variables?

5. (a) Show that '+' can be written in terms of negation (complement) and multiplication.
   (b) Can negation (i.e., complement) be written in terms of adding and multiplication?

2 Tutorial questions that your tutor will work through

This section contains problems that your tutor will work through with you during your tutorial class.

1. Compute $775^{20} \bmod 5381$, by first computing the binary expansion of 20, and using it as shown in lectures.
   Hence, or otherwise, determine the minimum positive integer power d such that $775^d \equiv 1 \pmod{5381}$.
   Given that 5381 is a prime number, what can you say about d and $\varphi(5381)$, where φ is the Euler φ-function.

   In DMTH237, we'll give a name to this concept of minimal power giving 1.
   Nevertheless, this idea will come in useful in some of the following exercises.

2. (a) Express the decimal number 8392 in binary notation.
   (b) Compute $241^{8392} \bmod 257$.
   (It's not nearly as difficult as it seems: notice that $241 = 257 - 16$ and $16^2 = 256$.)
   (c) Compute $225^{8392} \bmod 257$. (Notice that $225 = 257 - 32$ and $32^2 = 1024 = 4 \times 257 - 4$.)
   (d) At what power d did you realise that the calculation could be simplified?
   Find the prime decomposition of 257. How does d relate to $\varphi(257)$, where φ is the Euler φ-function?

3. Compute $749^{8392} \bmod 3329$.
   At what power d did you realise that the calculation could be simplified?
   Find the prime decomposition of 3329. How does d relate to $\varphi(3329)$, where φ is the Euler φ-function?

4. Can you compute $426861^{8392} \pmod{855553}$? Do not attempt this question before doing the earlier ones!!
   (HINT: try 257×3329.)

5. For the following table of a Boolean function of x and y write down a formula for $f(x, y)$ in *disjunctive normal form* (a sum of products) and also a formula in *conjunctive normal form* (a product of sums).

x	y	$f(x, y)$
1	1	0
1	0	1
0	1	1
0	0	0

Starting with the CNF, use the laws of Boolean algebra to write it in DNF.

6. Find the disjunctive and conjunctive normal forms of the Boolean function $f(x, y, z) = xy + \bar{z}$.

7. Find the disjunctive and conjunctive normal forms of formulas $F(x, y, z) = x\,\bar{y}$ and $G(x, y, z) = x + y + \bar{z}$.

3 Additional problems

These are problems that students who would like something a little more challenging can try at home after the tutorial. Your tutor may discuss some of these problems in the tutorial if time permits.
Give exact integer answers wherever it is reasonable to do so.

1. (a) Compute $4089^{4096} \bmod 4097$.
   (b) Compute $2^{4096} \bmod 4097$.
   (c) What can you deduce from this about the number 4097?

2. Compute $2^{140} \bmod 2059$. Hence compute $2^{2058} \bmod 2059$, and determine whether 2059 is prime.

3. Here is an account, from *Discrete Mathematics* by Dierker and Voxman (1986), on the steps applied to a Karnaugh Map to obtain a minimal expression.

   - Circle all isolated 1s. These terms must be included in the minimal expression.
   - Locate the 1s adjacent to only one other 1, and circle each of these pairs.
   - Circle rectangular blocks of four 1s if the block is the unique rectangular block that includes some 1s not yet circled.
   - Circle rectangular blocks of eight 1s if the block is the unique rectangular block that includes some 1s not yet circled.
   - Circle the largest possible rectangular blocks (two, four or eight 1s) needed to cover the remaining uncircled 1s.

   Apply these steps, or use what has been shown in lectures, to minimize the following expressions.
   Is there a unique result? (The wikipedia entry on Karnaugh maps is good.)

   - $E = wxyz + w\bar{x}y\bar{z} + \overline{w}\ \bar{x}y\bar{z} + \overline{w}xy\bar{z} + w\bar{x}\ \bar{y}\ \bar{z} + \overline{w}\ \bar{x}\ \bar{y}\ \bar{z} + \overline{w}x\bar{y}\ \bar{z} + w\bar{x}\ \bar{y}z$
   - $F = w\bar{x}yz + \overline{w}xyz + w\bar{x}y\bar{z} + \overline{w}\ \bar{x}y\bar{z} + \overline{w}xy\bar{z} + w\bar{x}\ \bar{y}\ \bar{z} + \overline{w}\ \bar{x}\ \bar{y}\ \bar{z} + \overline{w}x\bar{y}\ \bar{z} + w\bar{x}\ \bar{y}z + \overline{w}x\bar{y}z$