MACQUARIE University

DMTH137 – Session 2 – 2017

Week 13 Tutorial Exercises : Congruence Powers, Boolean Algebra

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?)

Answer: $0, 1, 11, 12, 16, 17, 6, 7, 8, 18, 19, 2, 3, 13, 14, 15, 4, 5, 9, 10, 20$.

This starts easily: $0^5 = 0$, $1^5 = 1$, $2^5 = 32 \equiv 11$, $3^5 = 243 \equiv 12$; then make use of earlier results (mod 21); *viz.* $4^5 = 2^5\,2^5 = 121 \equiv 16$, $5^5 \equiv 4 \times 4 \times 5 \equiv -4 \equiv 17$, $6^5 = 2^5\,3^5 \equiv 132 \equiv 6$, $7^2 = 49 \equiv 7$ so $7^5 \equiv 7$ also, $8^5 = 2^5\,4^5 = 11 \times 16 = 176 \equiv 8$, $9^5 = 3^5\,3^5 \equiv 144 \equiv 18$, $10^5 = 2^5\,5^5 \equiv 11 \times 17 = 187 \equiv 19$. To continue, just use negatives: $11^5 \equiv (-10)^5 \equiv -19 \equiv 2$, $12^5 \equiv -9^5 \equiv -18 \equiv 3$, $13^5 \equiv -8^5 \equiv -8 \equiv 13$, $14^5 \equiv -7^5 \equiv -7 \equiv 14$, $15^5 \equiv -6^5 \equiv -6 \equiv 15$, $16^5 \equiv -5^5 \equiv -17 \equiv 4$, $17^5 \equiv -4^5 \equiv -16 \equiv 5$, $18^5 \equiv -3^5 \equiv -12 \equiv 9$, $19^5 \equiv -2^5 = -11 \equiv 10$ and finally $20^5 \equiv -1^5 = -1 \equiv 20$.

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? **Answer**: $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20$.

After the trivial ones, use the results from the previous question: $0^{25} = 0$, $1^{25} = 1$, $2^{25} = (2^5)^5 \equiv 11^5 \equiv 2$, $3^{25} = (3^5)^5 \equiv 12^5 \equiv 3, \ldots$. Hold on, a minute!

We have for the Euler φ-function, that $\varphi(21) = \varphi(3)\,\varphi(7) = 2 \times 6 = 12$, and $25 = 2 \times 12 + 1$. So we see that $a^{25} = a^{2\times 12+1} \equiv a \pmod{21}$ for all a relatively prime to 21. We have just checked that $3^{25} \equiv 3$, and $7^5 \equiv 7$ so also $7^{25} \equiv 7$. Thus we'll have that $a^{25} \equiv a \pmod{21}$ for all $0 \le a \le 20$ (including multiples of 3 and 7).

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).

Answer: $F(x, y, z) = x\,y\,\bar{z} + x\,\bar{y}\,\bar{z} + \bar{x}\,\bar{y}\,z + \bar{x}\,\bar{y}\,\bar{z}$.

Conjunctive normal form gives a longer expression: $F(x, y, z) = (\bar{x} + \bar{y} + \bar{z})(\bar{x} + y + \bar{z})(x + \bar{y} + \bar{z})(x + \bar{y} + z)$.

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? **Answer**: $2^4 = 16$.

5. (a) Show that '+' can be written in terms of negation (complement) and multiplication.

Answer: $x + y = \overline{\bar{x} \cdot \bar{y}}$.

(b) Can negation (i.e., complement) be written in terms of adding and multiplication?

Answer: No, it cannot.

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 $775^d \equiv 1 \pmod{5381}$.

   Solution: In binary, we have $20 = 10100_2$ so we calculate the powers 755^2, 755^5, 755^{10} and 755^{20} modulo 5381. These are $775^2 \equiv 3334$, $775^5 \equiv 5380 \equiv -1 \pmod{5381}$, so clearly $775^{10} \equiv 1 \pmod{5381}$, so also $775^{20} \equiv 1$. It must be that 10 is the minimal power giving 1, since we know that neither 775^2 nor 775^5 are equivalent to 1.

   Given that 5381 is a prime number, what can you say about d and $\varphi(5381)$, where φ is the Euler φ-function.
   Solution: Since we know from theory that $a^{\varphi(5381)} \equiv 1$, and we have seen here that $775^{10} \equiv 1$, then it must be that $10 \mid \varphi(5381)$. If 5381 is prime, as claimed, then $\varphi(5381) = 5380$ which is indeed a multiple of 10. More generally, if $a^d \equiv 1 \mod n$ is the minimal such power giving 1, then it must be that $d \mid \varphi(n)$.

   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. **Answer**: $8392 = 10000011001000_2$.

   (b) Compute $241^{8392} \mod 257$.
   (It's not nearly as difficult as it seems: notice that $241 = 257 - 16$ and $16^2 = 256$.) **Answer**: 1.
   $241^2 \equiv (-16)^2 = 16^2 = 256 \equiv -1 \mod 257$. So the numbers calculated as powers are: 241, −1, 1, 1, 1, 1, 241, −241, −1, 1, 241, −1, 1, finishing with 1.

   (c) Compute $225^{8392} \mod 257$. (Notice that $225 = 257 - 32$ and $32^2 = 1024 = 4 \times 257 - 4$.)
   Answer: $-1 \equiv 256 \mod 257$.
   The numbers calculated as powers are: 225, −4, 16, −1, 1, 1, 225, 128, 193, 241, −225, −4, 16 and finally we get −1. Notice that $225^{16} \equiv 1 \mod 257$.

   (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?
   Solution: With $225^{16} \equiv 1 \mod 257$, but 225^{2^k} not equivalent to 1, for $k < 4$, then $d = 16$ must be the minimal power. Thus we could simplify the calculation by observing that $8392 = 524 \times 16 + 8$. So $225^{8392} = 225^{524 \times 16 + 8} \equiv 225^8 \equiv -1 \mod 257$, as was calculated earlier. Note that since 257 is prime, then $\phi(257) = 256 = 2^8$. Thus minimum powers giving 1 modulo 257 must be powers of 2; here we have found 16 for 225 and 4 for 241.

3. Compute $749^{8392} \mod 3329$. **Answer**: $1 \mod 3329$.
   In binary we have $8392 = 10000011001000_2$, so we calculate powers. Starting out, we find: $749^2 \equiv 1729$, $749^4 \equiv -1$, so that $749^8 \equiv 1$. But $8392 = 1049 \times 8$, so we have $(749^8)^{1049} = 1^{1049} \equiv 1 \mod 3329$.

   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?

   Solution: We found $749^8 \equiv 1$, after just 3 congruence multiplications. Now 3329 is prime, so we have that $\varphi(3329) = 3328 = 2^8 \times 13$. The minimum power $d = 8$ is a divisor of $\varphi(3329)$, as expected.

4. Can you compute $426861^{8392} \pmod{855553}$? Do not attempt this question before doing the earlier ones!!
   (Hint: try 257×3329.) **Answer**: $1 \mod 855553$.
   First note that $257 \times 3329 = 855553$, so we can use previous results found for the primes 257 and 3329. That is, reducing modulo 257 we find $426861 \equiv 241 \pmod{257}$, and that $426861 \equiv 749 \pmod{3329}$.
   Now we already know that $426861^{8392} \equiv 241^{8392} \equiv 1 \pmod{257}$, and $426861^{8392} \equiv 749^{8392} \equiv 1 \pmod{3329}$. By the Chinese Remainder Theorem, or other solution method, the double congruence $x \equiv 1 \pmod{257}$ and $x \equiv 1 \pmod{3329}$ has a solution of $x \equiv 1 \pmod{855553}$.

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

   Answer: DNF: $x\bar{y} + \bar{x}y$ CNF: $(\bar{x} + \bar{y})(x + y)$.

   Starting with the CNF, use the laws of Boolean algebra to write it in DNF.
   Solution: $(\bar{x} + \bar{y})(x + y) = \bar{x}x + \bar{x}y + \bar{y}x + \bar{y}y = 0 + \bar{x}y + x\bar{y} + 0 = \bar{x}y + x\bar{y}$.

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

$f(x,y,z) = xy + \bar{z} = xy(z+\bar{z}) + (x+\bar{x})(y+\bar{y})\bar{z} = xyz + xy\bar{z} + (xy\bar{z} + x\bar{y}\bar{z} + \bar{x}y\bar{z} + \bar{x}\bar{y}\bar{z}) = xyz + xy\bar{z} + x\bar{y}\bar{z} + \bar{x}y\bar{z} + \bar{x}\bar{y}\bar{z}$. CNF: $f(x,y,z) = (x+y+\bar{z})(x+\bar{y}+\bar{z})(\bar{x}+y+\bar{z})$, since $f(x,y,z) = 0$ for $(x,y,z) \in \{(0,0,1),(0,1,1),(1,0,1)\}$.

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

DNF: $F(x,y,z) = x\,\bar{y} = x\,\bar{y}\,(z+\bar{z}) = x\,\bar{y}\,z + x\,\bar{y}\,\bar{z}$.

$G(x,y,z) = x+y+\bar{z} = x(y+\bar{y})(z+\bar{z}) + (x+\bar{x})y(z+\bar{z}) + (x+\bar{x})(y+\bar{y})\bar{z}$
$= (xyz + xy\bar{z} + x\bar{y}z + x\bar{y}\bar{z}) + (xyz + xy\bar{z} + \bar{x}yz + \bar{x}y\bar{z}) + (xy\bar{z} + x\bar{y}\bar{z} + \bar{x}y\bar{z} + \bar{x}\bar{y}\bar{z})$
$= xyz + xy\bar{z} + x\bar{y}z + x\bar{y}\bar{z} + \bar{x}yz + \bar{x}y\bar{z} + \bar{x}\bar{y}\bar{z}$.

CNF: $F(x,y,z) = (x+y)(x+\bar{y})(\bar{x}+\bar{y}) = (x+y+z)(x+y+\bar{z})(x+\bar{y}+z)(x+\bar{y}+\bar{z})(\bar{x}+\bar{y}+z)(\bar{x}+\bar{y}+\bar{z})$.

$G(x,y,z) = x+y+\bar{z}$ is already in CNF.

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 $4089^{4096} \bmod 4097$. **Answer**: $1 \pmod{4097}$.

With $4096 = 2^{12} = 1000000000000_2$, we just need squaring. We find that $4089^2 \equiv 64 = 2^6$, then $4089^4 \equiv 2^{12} \equiv -1 \pmod{4097}$. Thus $4089^8 \equiv 1 \pmod{4097}$, and further squaring will not change this. Hence $4089^{4096} \equiv 1 \pmod{4097}$.

(b) Compute $2^{4096} \bmod 4097$. **Answer**: -16.

Repeated squaring gives $2, 4, 16, 256, -16, 256, \ldots$. The numbers just alternate between -16 and 256 with further squaring. In particular $2^{4096} \not\equiv 1 \pmod{4097}$.

(c) What can you deduce from this about the number 4097? **Answer**: not a prime.

It cannot be the case that $\varphi(4097)$ is 4096, so 4097 is not a prime. In fact, $4097 = 17 \times 241$.

2. Compute $2^{140} \bmod 2059$. **Answer**: $1 \bmod 2059$.

Hence compute $2^{2058} \bmod 2059$, and determine whether 2059 is prime. **Answer**: $289 \bmod 2059$.

We have that $2058 = 15 \times 140 + 98$, so we only need to calculate $2^{98} \bmod 2059$. In binary, $98 = 1100010_2$ giving powers: $3, 6, 12, 24, 49, 98$. The numbers are: $8, 64, 2037, 484, 1119, 289$. Since $2^{2058} \not\equiv 1 \pmod{2059}$, it cannot be that 2059 is prime. In fact, $2059 = 29 \times 71$.

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.)

- $E = wxyz + w\bar{x}y\bar{z} + \overline{w}\;\overline{x}yz + \overline{w}xy\bar{z} + w\bar{x}\;\overline{y}\;\overline{z} + \overline{w}\;\overline{x}\;\overline{y}\;\overline{z} + \overline{w}x\overline{y}\;\overline{z} + w\bar{x}\;\overline{y}z$
Answer: $E(w,x,y,z) = \bar{x}\bar{z} + \bar{w}\bar{z} + w\bar{x}\bar{y} + wxyz$.

See the Karnaugh map at left below.

E	$y\,z$	$y\,\bar{z}$	$\bar{y}\,\bar{z}$	$\bar{y}\,z$
$w\,x$	1			
$w\,\bar{x}$		1	1	1
$\bar{w}\,\bar{x}$		1	1	
$\bar{w}\,x$		1	1	

F	$y\,z$	$y\,\bar{z}$	$\bar{y}\,\bar{z}$	$\bar{y}\,z$
$w\,x$				
$w\,\bar{x}$	1	1	1	1
$\bar{w}\,\bar{x}$		1	1	
$\bar{w}\,x$	1	1	1	1

- $F = w\overline{x}yz + \overline{w}xyz + w\bar{x}y\bar{z} + \overline{w}\;\overline{x}y\overline{z} + \overline{w}xy\overline{z} + w\bar{x}\;\overline{y}\;\overline{z} + \overline{w}\;\overline{x}\;\overline{y}\;\overline{z} + \overline{w}x\overline{y}\;\overline{z} + w\bar{x}\;\overline{y}z + \overline{w}x\overline{y}z$
Answer: not unique: $F(w,x,y,z) = w\bar{x} + \bar{w}x + \bar{x}\bar{z} = w\bar{x} + \bar{w}x + \bar{w}\bar{z}$.

See the Karnaugh map at right above: requires one of the middle circles, but not both.