UNIVERSITY OF WATERLOO

Faculty of Mathematics
Waterloo, Ontario N2L 3G1

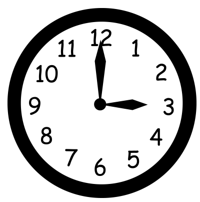
Centre for Education in
Mathematics and Computing

Grade 7/8 Math Circles

February 9-10, 2016

Modular Arithmetic

1 Introduction: The 12-hour Clock



Question: If it's 7 pm now, what time will it be in 7 hours? 2 am

How about in 30 hours? 1 am after tomorrow

Now, this is a simple example that we're all familiar with, but how did we actually calculate this? Can you simplify this into 2 or 3 simple steps?

① Add 7 (time it is now) to 7 or 30 (number we're asked to add).

② Keep subtracting 12 from this sum until you get a number less than 12.

2 Review of Divisibility

Definition: An integer x is divisible by an integer n if $x \div n$ is an integer *(ie. there is no remainder when x is divided by n)*. We write $x \mid n$, which is read "x is divisible by n".

Can you think of another way to ask "Is x divisible by n?"

Exercise 1

(a) Is 15 divisible by 3? Yes

(b) Is 75 divisible by 2? No

Note: this is another way of asking if 75 is even

(c) Is 50 divisible by 15? No

(d) is 150 divisible by 3? Yes

3 Modular Operator

The modular operator might seem a little intimidating at first, but it's really not. All it does is, given 2 integers (x and n), it produces the remainder when the first number is divided by the second.
Notation: $x \pmod{n} = r$
This means that when x is divided by n, there is a remainder of r.
We say: "x modulo n is equal to r".

Examples:

(a) $7 \pmod 4 = 3$

(b) $15 \pmod 3 = 0$

(c) $19 \pmod 4 = 3$

(d) $21 \pmod 5 = 1$

Exercise 2: Calculate each of the following.

(a) $7 \pmod 5 = 2$

(b) $8 \pmod 4 = 0$

(c) $8 \pmod 3 = 2$

(d) $17 \pmod 8 = 1$

(e) $37 \pmod 6 = 1$

(f) $124 \pmod{60} = 4$

3.1 Modular Addition

Modular addition is actually quite straight forward.
For example:

$$(1+2) \pmod 4 = 3$$
$$(4+5) \pmod 5 = 9 \pmod 5 = 4$$

Pretty simple right? What if it got more complicated though, like this one?

$$(187468 + 847361) \pmod 2 = \underline{\hspace{2cm}}$$

This is not an easy calculation, unless you have a calculator, but that defeats the purpose of modular arithmetic, which is to simplify complicated calculations.
So, we propose an idea: What if we were to calculate each number with respect to that modulo before we add them together? Now this complicated question becomes really simple:

$$(187468 + 847361) \pmod 2 = (0 + 1) \pmod 2 = 1$$

The next natural thought would be to define modular addition as the following:

$$(x+y) \pmod n = x \pmod n + y \pmod n$$

For example: $(7+6) \pmod 5 = 7 \pmod 5 + 6 \pmod 5 = (2+1) \pmod 5 = 3$

Try this one: $(19{+}28) \pmod 5 = \underline{19 \pmod 5 + 28 \pmod 5 = (4+3) \pmod 5 = 7 \pmod 5 = 2}$

As we see with this example, we can't just calculate each number with respect to $\pmod n$ and add them together, sometimes we are required to simplify the sum in with respect to $\pmod n$ after we sum them. So we define modular addition as:

$$\boxed{(x+y) \pmod n = [x \pmod n + y \pmod n] \pmod n}$$

In general, we know we've simplified it as much as possible when the result is <u>less that n.</u>

Exercise 3: Calculate each of the following.

(a) $5+9 \pmod 8 = 5+1 \pmod 8 = 6$

(b) $43+37 \pmod{10} = 3+7 \pmod{10} = 10 \pmod{10} = 0$

(c) $124+199 \pmod 5 = 4+4 \pmod 5 = 8 \pmod 5 = 3$

(d) $34+121 \pmod{11} = 1+0 \pmod{11} = 1$

3.2 Modular Multiplication

Modular multiplication is very similar to modular addition. We define it as:

$$\boxed{(x \times y) \pmod n = [x \pmod n \times y \pmod n] \pmod n}$$

Exercise 4: Calculate each of the following.

(a) $5 \times 9 \pmod 8 = 5 \times 1 \pmod 8 = 5$

(b) $7 \times 15 \pmod 7 = 0 \times 1 \pmod 9 = 0$

(c) $5782 \times 2579 \pmod{10} = 2 \times 9 \pmod{10} = 18 \pmod{10} = 8$

(d) $603 \times 123 \pmod{60} = 3 \times 3 \pmod{60} = 9$

(e) $16 \times 25 \pmod{12} = 4 \times 1 \pmod{12} = 4$

(f) $34 \times 122 \pmod{11} = 1 \times 1 \pmod{11} = 1$

4 Common Bases

Modular artihmetic are used in the real world on a daily basis. As we saw in the introduction of this lesson, base 12 is a common one used in analog clocks. Here are some other commonly used bases:

Base	**Application**	**Example**
2	Even/odd numbers Binary codes	A number n is even if $n \pmod 2 = 0$, and odd otherwise. We also use base 2 when using converting from binary to decimal form, as we will see later.
4	Years between 2 consecutive leap years (in general)	If any given year n is either $[n \pmod{400} = 0]$ or $[n \pmod 4 = 0$ and $n \pmod{100} \neq 0]$ then it is a leap year, otherwise it isn't.
7	Days in a week	If today is Sunday, then in 16 days it will be a Tuesday (since $16 \pmod 7 = 2$).
10	Metric measurements	We use base 10 when converting between metric measurments, such as metres to millimetres.
12	Hours on an analog clock	If it's 7 pm now, it will be 2 am in 7 hours (since $(7+7) \pmod{12} = 14 \pmod{12} = 2$).
24	Hours in a day	If its 2 pm now, in 54 hours it will be 8 am (since $(54+2) \pmod{24} = 8$).
28, 29, 30, 31	Days in a month	If today is the 4^{th} of April, then it will be the 8^{th} of May in 34 days.
52	Weeks in a year	If today is the 6^{th} week of the year, then it will be the 16^{th} week of next year in 62 weeks.
60	Seconds in a minute and minutes in an hour	155 seconds is equivalent to 2 minutes and 35 seconds.
100	Years in a century	In 344 years, it will be the 60^{th} year of that century, since $(344+2016) \pmod{100} = 60$.
360	Degrees in a full circle	Rotating 420° is equivalent to rotating 60° since $420 \pmod{360} = 60$.
365	Days in a year	If today is the 65^{th} day of the year, then in 750 days, it will be 85^{th} day of that year.

5 Binary Numbers and Codes

A binary code is any system that only uses 2 states: 1/0, on/off, true/false etc.
A binary number is any number containing only 1's and 0's. These are all examples of binary numbers:

101 000000 1111111 10001001010010 10001111101010 0101010101010

Binary numbers have all sorts of applications, many of which are used on a daily basis, like:

- Computers
- Calculators
- TV's
- Barcodes
- CD's and DVD's
- Braille

Binary codes are also used in many work fields, such as computer science, software engineering and electrical engineering - and basically all other fields of engineering too!
There are multiple ways to express a binary code, the two most common forms of writing a binary code using numbers are 'Decimal form' and 'Binary form'.
For example: 1101 in binary form becomes 13 in decimal form. And 1001 becomes 9.
Now, the conversion between these may not be obvious, but it's pretty easy. Before we jump into converting between binary and decimal forms, let's do a quick review on exponents:

$$x^0 = 1$$
$$x^1 = x$$
$$x^2 = x \times x$$
$$x^3 = x \times x \times x$$
$$x^4 = x \times x \times x \times x$$
$$x^5 = x \times x \times x \times x \times x$$

and so on... (for any x)

Also, fill out this table, it will be very useful for the rest of the lesson.

n	0	1	2	3	4	5	6	7	8
2^n	$2^0 = 1$	$2^1 = 2$	$2^2 = 4$	$2^3 = 8$	$2^4 = 16$	$2^5 = 32$	$2^6 = 64$	$2^7 = 128$	$2^8 = 256$

5.1 Converting Binary to Decimal

To convert a binary number to its decimal form, follow these 3 simple steps:

① Write out the number - but leave lots of space between your digits, like this:

$$1 \qquad\qquad 0 \qquad\qquad 0 \qquad\qquad 1$$

② Multiply each number by a 2, and starting with an exponent of 0 on the very last 2, and increase the exponent by 1 each time, like this:

$$[1 \times (2^3)] \quad [0 \times (2^2)] \quad [0 \times (2^1)] \quad [1 \times (2^0)]$$

③ Sum them up and calculate:

$$[1 \times (2^3)] + [0 \times (2^2)] + [0 \times (2^1)] + [1 \times (2^0)]$$

$$=[1 \times (8)] + [0 \times (4)] + [0 \times (2)] + [1 \times (1)]$$

$$=8 + 0 + 0 + 1 = 9$$

Exercise 5: Convert each of the follwing binary numbers to decimal form.

(a) $110 \rightarrow 1(2^2) + 1(2^1) + 0(2^0) = 4 + 2 + 0 = 6$

(b) $101 \rightarrow 1(2^2) + 0(2^1) + 1(2^0) = 4 + 0 + 1 = 5$

(c) $00111 \rightarrow 0(2^4) + 0(2^3) + 1(2^2) + 1(2^1) + 1(2^0) = 4 + 2 + 1 = 7$

(d) $100001 \rightarrow 1(2^5) + 0 + 0 + 0 + 0 + 1(2^0) = 32 + 1 = 33$

5.2 Converting Decimal to Binary

Now this is the part where modular arithmetic comes in handy!
We know that if we compute any number (mod 2) it will either be 0 or 1, and so that's exactly what we use for converting decimal numbers to binary.
Basically, we compute our number (mod 2) and that will be our last digit. Then we compute our quotient (mod 2) and place that as our 2^{nd} last digit, and so on until our quotient is 0.
For example: Converting 13 to binary form, we would do the following.

$$\begin{aligned}
13 &= 2(6) + 1 \quad \Rightarrow \quad 13 \pmod 2 = 1 \\
6 &= 2(3) + 0 \quad \Rightarrow \quad 6 \pmod 2 = 0 \\
3 &= 2(1) + 1 \quad \Rightarrow \quad 3 \pmod 2 = 1 \\
1 &= 2(0) + 1 \quad \Rightarrow \quad 1 \pmod 2 = 1
\end{aligned}$$

Now reading from the bottom up, 13 in decimal form is 1101 in binary form.
Note: Your last step should ALWAYS be the same as the one above.
Exercise 6: Convert each of the following numbers to binary form.

(a) 76

$76 = 2(38) + 0$
$38 = 2(19) + 0$
$19 = 2(9) + 1$
$9 = 2(4) + 1$
$4 = 2(2) + 0$
$2 = 2(1) + 0$
$1 = 2(0) + 1$
$\Rightarrow 1001100$

(b) 193

$193 = 2(96) + 1$
$96 = 2(48) + 0$
$48 = 2(24) + 0$
$24 = 2(12) + 0$
$12 = 2(6) + 0$
$6 = 2(3) + 0$
$3 = 2(1) + 1$
$1 = 2(0) + 1$
$\Rightarrow 11000001$

(c) 97

$97 = 2(48) + 1$
$48 = 2(24) + 0$
$24 = 2(12) + 0$
$12 = 2(6) + 0$
$6 = 2(3) + 0$
$3 = 2(1) + 1$
$1 = 2(0) + 1$
$\Rightarrow 1100001$

(d) 255

$255 = 2(127) + 1$
$127 = 2(63) + 1$
$63 = 2(31) + 1$
$31 = 2(15) + 1$
$15 = 2(7) + 1$
$7 = 2(3) + 1$
$3 = 2(1) + 1$
$1 = 2(0) + 1$
$\Rightarrow 11111111$

6 Problem Set

1. Calculate each of the following

   (a) $100 \pmod 3 = 1$

   (b) $451 \pmod 5 = 1$

   (c) $490 \pmod 7 = 0$

   (d) $234 \pmod 4 = 2$

   (e) $478 \pmod 6 = 4$

   (f) $582 \pmod 9 = 540 \pmod 9 + 42 \pmod 9 = 6$

   (g) $679 \pmod 8 = 640 \pmod 8 + 39 \pmod 8 = 7$

   (h) $12 + 18 \pmod 9 = 4$

   (i) $73 + 58 \pmod{12} = 1 + 10 \pmod{12} = 11$

   (j) $74 \times 93 \pmod{13} = 9 \times 2 \pmod{13} = 18 \pmod{13} = 5$

   (k) $33 \times 266 \pmod{26} = 7 \times 6 \pmod{26} = 42 \pmod{26} = 16$

2. Complete the following table by either converting the given binary number to decimal form or vice versa.

	Binary	Decimal
(a)	0101	5
(b)	100111	39
(c)	1111	15
(d)	10100	20
(e)	1010101	85
(f)	10010110	150
(g)	101101	45
(h)	111011	59

3. If my birthday was on Monday, January 5, 2015, what day of the week will my birthday be on this year (2016)?
   $365 \pmod 7 = 350 \pmod 7 + 15 \pmod 7 = 0 + 1 \pmod 7 = 1$
   $\therefore$ My birthday would have been on Tuesday, January 5^{th}, 2016.

4. If Mary's birthday was on a Thursday in 2014, what day of the week will her birthday be on next year (2017)?
   $[(365 \times 2) + 366] \pmod 7 = (1 \times 2) \pmod 7 + 2 \pmod 7 = 2 + 2 \pmod 7 = 4$
   $\therefore$ Mary's birthday would have been on a Monday, since that is 4 days after Thursday.

5. Using a regular deck of 52 cards, I dealt all the cards in the deck to 3 people (including myself). Were the cards dealt evenly?
   $52 \pmod 3 = 1$
   $\therefore$ No, it wasn't dealt evenly.

6. A litre of milk is 4 cups, and one cake recipe uses 3 cups. If I have 8 litres of milk, how many cakes can I make? And how many cups of milk will be leftover, if any?
   $8 \times 4 \pmod 3 = 2 \times 1 \pmod 3 = 2$
   $\frac{(8\times4)-2}{3} = \frac{32-2}{3} = \frac{30}{3} = 10$
   $\therefore$ I will be able to make 10 cakes with 2L of milk leftover.

7. I bought as many mini-erasers as possible at 25 cents each and spent the rest of my money on paperclips at 3 cents each. How many of each did I buy given that I have \$1.70? Is there anything leftover? *(Assume there's no tax.)*
   Maximum amount of money I can spend on erasers is \$1.50, getting me 6 erasers and leaving me with \$0.20 to buy paper clips.
   $20 \pmod 3 = 2$ and since $20 = 3(6) + 2$
   $\therefore$ I can buy 6 erasers and 6 paperclips, and would have 2¢ leftover.

8. I have 5 trays with 6 muffins each that I divided evenly among 4 of my friends, and I ate the leftovers. How many muffins did each of my friends eat? How many muffins did I eat?
   $5 \times 6 = 30 = 7(4) + 2$
   $\therefore$ Each of my friends ate 7 and I ate 2.

9. If Math Circles started on Tuesday, February 2^{nd}, 2016, and lasts for 44 days, what day will it end? *(Give the full date.)*
   Note that 44 us NOT *the number of classes there are, rather it is the number of days in between the first and last day of Math Circles.*
   $44+2 \pmod{29} = 15+2 \pmod{29} = 17 \implies$ *So it will fall on the* 17^{th} *day of March.*
   $44 \pmod 7 = 2 \implies$ *So it will fall 2 days after Tuesday, ie. it will fall on a Thursday.*
   $\therefore$ The last day will be Thursday, March 17^{th}, 2016.

10. If John celebrated his 16^{th} birthday on Wednesday, February 10^{th}, 2016, what day of the week was he born? *(Don't forget about leap years!)*

Clearly John was born in the year 2000. Since his birthday is before February 29^{th}, he would have lived through 4 leap years (2000, 2004, 2008 and 2012) and 12 years with 365 days each. So we want to calculate:

$[(365 \times 12) + (366 \times 4)] \pmod 7 = [(1 \times 5) + +(2 \times 4)] \pmod 7 = 5 + 8 \pmod 7 = 6$

This means that his 16^{th} birthday fell 6 days (in the week) after the day on which he was born.

So if we work backwards, 6 days before Wednesday is Thursday.

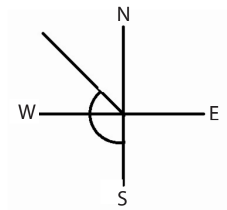
$\therefore$ John was born on Thursday, February 10^{th}, 2000.

11. Mary is facing South and rotates 2295° clockwise. Which direction is she facing now?

We want to know how many degrees she rotated CW from South. So we calculate:

$2295 \pmod{360} = 135$

$\therefore$ Mary rotated 135°clockwise and so she would be facing North-West.



12. (a) How many different 5-digit binary numbers are there?

Solution 1:

We will first approach this question by looking into how many possibilities there are for each of the 5 digits.

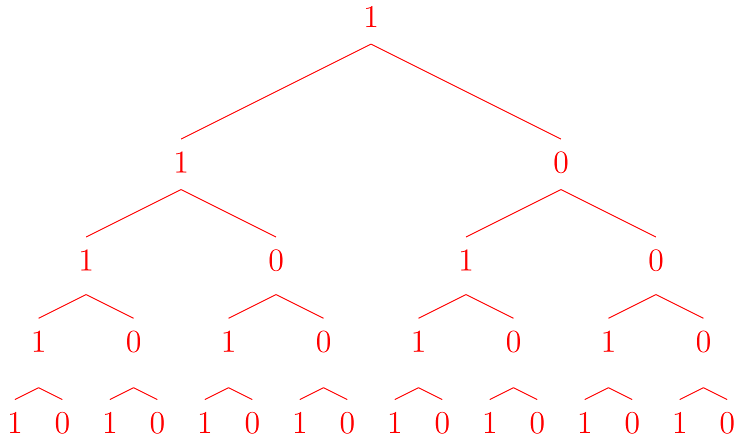
1	1 0	1 0	1 0	1 0

$1 \quad \times \quad 2 \quad \times \quad 2 \quad \times \quad 2 \quad \times \quad 2 \quad = \quad 16$

Notice that the only possible number in the first digit is 1, if it were 0 it would be considered a 4-digit binary number.

Solution 2:

We can also approach this question by drawing a tree where the first level represents the first digit, which can only be filled by a 1. The second row represents the second digit which can be filled with a 1 or 0 and so on.



Counting the number of nodes on the last row, we get an answer of 16.

(b) How many different 5-digit binary numbers are there that have 1 as the last digit?

Solution 1:

Using a similar table from part (a), we have the following:

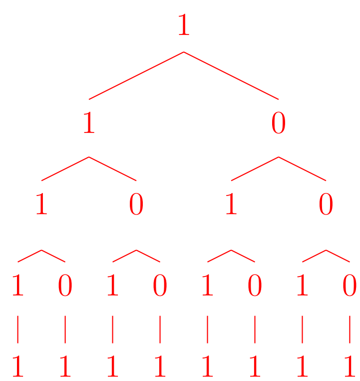
1	1 0	1 0	1 0	1

$$1 \times 2 \times 2 \times 2 \times 1 = 8$$

Notice that it is just half of our answer in part (a), because half of the possible 5-digit numbers end in 1 and the other half end in 0.

Solution 2:

A tree for this question would look something like this:



Counting the number of nodes on the fifth level, we get an answer of 8.

13. Look back at the table titled "Common Bases"

(a) Was the year 1900 a leap year?

We will calculate 1900 modulo 4, 100 and 400 to test if it was a leap year or not.

$$1900 \pmod 4 = 0$$
$$1900 \pmod{100} = 0$$
$$1900 \pmod{400} = 300$$

$\therefore$ No, 1900 wasn't a leap year, since $1900 \pmod 4 = 0$ and $1900 \pmod{100} = 0$ but $1900 \pmod{400} \neq 0$

(b) Was the year 2000 a leap year?

Similarily, we will calculate 2000 modulo 4, 100 and 400 to test if it was a leap year or not.

$$2000 \pmod 4 = 0$$
$$2000 \pmod{100} = 0$$
$$2000 \pmod{400} = 0$$

$\therefore$ Yes, 2000 was a leap year.

(c) Is the year 2100 going to be a leap year?

We will calculate 2100 modulo 4, 100 and 400 to test if it will be a leap year or not.

$$2100 \pmod 4 = 0$$
$$2100 \pmod{100} = 0$$
$$2100 \pmod{400} = 100$$

$\therefore$ No, 2100 will not be a leap year.

(d) Is the year 2200 going to be a leap year?

We will calculate 2200 modulo 4, 100 and 400 to test if it will be a leap year or not.

$$2200 \pmod 4 = 0$$
$$2200 \pmod{100} = 0$$
$$2200 \pmod{400} = 200$$

$\therefore$ No, 2200 will not be a leap year.

14. There are seven stacks of coins that look the same. Each stack has exactly 100 coins. There are two stacks that have counterfeit coins, and all 100 coins in each of those two stacks are counterfeit. Your task is to figure out which two of the seven stacks contain the counterfeit coins.

    The counterfeit coins weigh 11g each, while the real coins weigh 10g each. You have an electric balance, but you can only use it to make one measurement.

    How can you determine which two stacks contain the counterfeit coins with only one use of the balance? Explain why the strategy works.

    (Hint: Think about taking different numbers of coins from each of the stacks and placing them on the balance together. Think about the important numbers in the binary number system.)

    We would like to take a different number of coins from each stack so that we know which stacks have the counterfeit coins. If the question had just 1 counterfeit coin pile, then we could just take 1 from the first, 2 from the second, 3 from the third and so on.

    Note: if there were no counferfeit coins, the total weight taking one from the first pile and 2 from the second and so on would be $\frac{(7)(7+1)}{2} = 28$.

    However we cannot do that this time, because we wouldn't be able to know for sure which piles had the counterfeit coins.

    For example if the total weight was 33, then there could be 2 possibilities including the 1^{st} and 4^{th} or 2^{nd} and 3^{rd}. But we want to avoid these ambiguous situations.

    To do this, we basically want to write a 7-digit binary number with two 1's.

    From the 1^{st} stack, we take $2^0 = 1$.

    From the 2^{nd} stack, we take $2^1 = 2$.

    From the 3^{rd} stack, we take $2^2 = 4$ and so on until you take $2^6 = 64$.

    Then when you weigh them, and convert this number in decimal form to binary form, and from the position of the two 1's you can easily determine which piles contains the counterfeit coins.