Modular Arithmetic

Summary

This lesson is an exploration of modular arithmetic. It starts with some occurrences of patterns in powers of numbers and in clock arithmetic.

Resources

- 1 Question Sheet per student.
- 1 Modular Arithmetic Rules sheet

Questions/Suggestions?

If you plan to use this material, or if you would write to send us feedback, please email a.mustata@ucc.ie

References:

-Fomin, S. Genkin, I. Itenberg “Mathematical Circles (Russian Experience)”

-Cut-the-Knot website

Modular Arithmetic

1. Digit Patterns

Find the last digit of each of the following numbers:

$(i)\ 9^{2016}$

n	Last digit of 9^n
1	
2	
3	
4	
5	
	.....
2016	

$(ii)\ 7^{2016}$

n	Last digit of 7^n
1	
2	
3	
4	
5	
	.....
2016	

2. Time patterns:

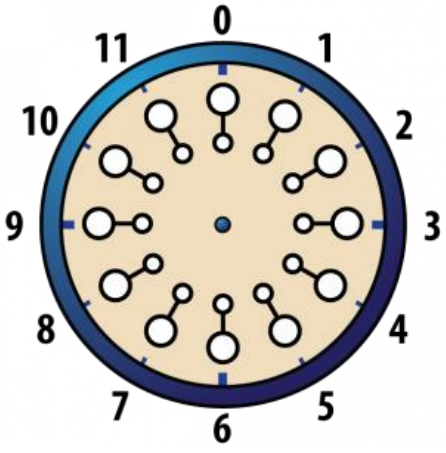
When two lengths of time A and A' are represented in the same way by the clock, we say

$$A = A' \ (mod\ 12).$$

$A = A' \ (mod\ 12)$ if $A \div 12$ and $a \div 12$ give the same reminders, or, equivalently,

$A - A' = 12 \times k$ for some integer k.

3. Arithmetic around the clock



a) At 00:00 on New Year, my friend Aoife will start a trip around the country which is to last exactly 42 hours. What time will the clock show at the end of her trip?

b) At 00:00 on New Year, my friend Saoirse will start a trip around the country which is to last exactly 26 hours. What time will the clock show at the end of her trip?

c) Immediately after arriving back from her 42 hour trip, Aoife hears of Soirse's itinerary and she immediately sets on a similar 26 hour trip. What time will the clock show when she finishes her trip?

d) I also start at 00:00 on New Year, and my trip is split into 5 sections of 26 hours each. What time will the clock show at the end of my trip? How about if I do 17 sections of 26 hours each?

$\mathbf{42} = 3 \times 12 + \mathbf{6}$	$\mathbf{26} = 2 \times 12 + \mathbf{2}$
$\mathbf{26} = 2 \times 12 + \mathbf{2}$	$\mathbf{17} = 1 \times 12 + \mathbf{5}$
$\mathbf{42} + \mathbf{26} = 5 \times 12 + \mathbf{8}$	$\mathbf{17} \times \mathbf{26} = (2 \times 12 + 2)(12 + 5) = 2 \times 12^2 + 2 \times 12 + 5 \times 12 + \mathbf{5} \times \mathbf{2}$

$$A \equiv A' \ (mod\ n)$$

means: $A - A'$ *is a multiple of* n

equivalently: $A = A' + k \times n$ for some integer k.

4. General Mod Arithmetic rules:

If $A_1 \equiv A_2 \ (mod\ n)$ **and** $B_1 \equiv B_2 \ (mod\ n)$ **then**

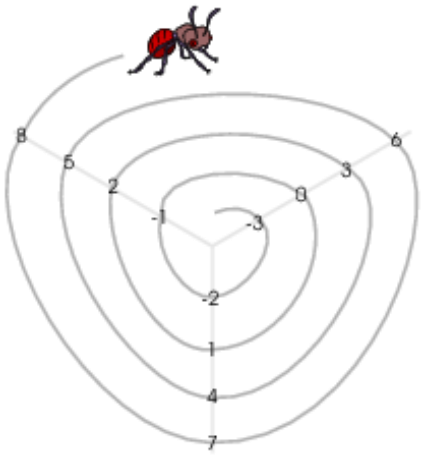
$$A_1 + B_1 \equiv A_2 + B_2 \ (mod\ n),$$

$$A_1 B_1 \equiv A_2 B_2 \ (mod\ n),$$

$$A_1^k \equiv A_2^k \ (mod\ n)$$

but in general $A_1^{B_1} \not\equiv A_2^{B_2} \ (mod\ n)$ **(exponent mods ≠ basis mods)**

5. Mod 3:



Calculate:

$a)\ 1 + 2 + 3 + 4 + 5 + \cdots + 2013 + 2014 \ (mod\ 3)$

$b)\ 2014^3 \ (mod\ 3)$=

$c)\ 7^{2016} \ (mod\ 3)$=

$d)\ 8^{2016} \ (mod\ 3)$=

Hint: all numbers are congruent to either 0, 1 or -1 mod 3.

$e)$ Prove that $x^3 - x$ is always a multiple of 3, no matter what integer number x we choose.

$f)$ Prove that $x^2 - 1$ is a multiple of 3 for all x which are not multiples of 3.

$g)\ 987654321^{2016} \ (mod\ 3)$ =

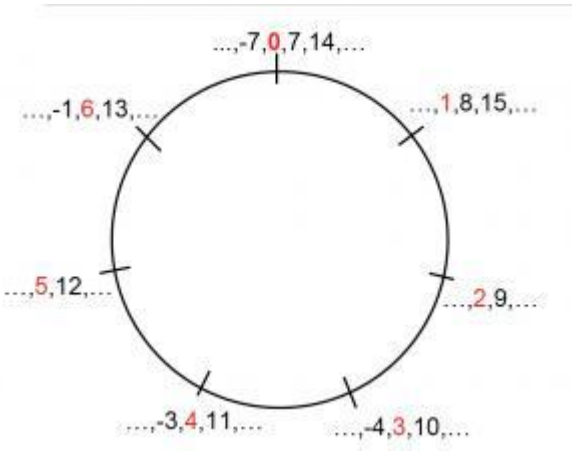
6. Mod 5:

a) Prove that $x^4 - 1$ is a multiple of 5 for all x which are not multiples of 5.

(Hint: take $x = 1,\ 2, -1, -2$)

b) $12345678^{2016} \ (mod\ 5) =$

7. Mod 7:



$2^1 \equiv$	$3^1 \equiv$	$4^1 \equiv$	$2016^1 \equiv$
$2^2 \equiv$	$3^2 \equiv$	$4^2 \equiv$	$2016^2 \equiv$
$2^3 \equiv$	$3^3 \equiv$	$4^3 \equiv$	$2016^3 \equiv$
$2^6 \equiv$	$3^6 \equiv$	$4^6 \equiv$	$2016^6 \equiv$
$2^{2016} \equiv$	$3^{2016} \equiv$	$4^{2016} \equiv$	$2016^{2016} \equiv$

7. Fermat's Little Theorem:

If p is a prime number and x is any number which is not a multiple of p, then

$$x^{p-1} \equiv 1 \pmod{p}.$$

Example: Alice is using the conversion table below and the encryption formula $x \to x^{19} \pmod{29}$.

Conversion Table

A = 1	K = 11	U = 21
B = 2	L = 12	V = 22
C = 3	M = 13	W = 23
D = 4	N = 14	X = 24
E = 5	O = 15	Y = 25
F = 6	P = 16	Z = 26
G = 7	Q = 17	
H = 8	R = 18	
I = 9	S = 19	
J = 10	T = 20	

to send Bob the following secret message:

18_5_1_19

What does she mean?

8. Euler's Theorem:

If n is any integer, we define $\varphi(n)$ =the number of items in the list $1, 2, 3, \dots, n-1$ which share no common factors with n.

If x is such a number, then

$$x^{\varphi(n)} \equiv 1 \pmod{n}.$$

Examples:

a) If n= prime, then $\varphi(n) = n - 1$.

b) If $n = pq$ where p, q are prime, then $\varphi(n) = (p-1)(q-1)$.

c) Alice and Bob are using the RSA decryption algorithm to communicate securely: Bob releases a public key which consists of the mod n = 91 and the exponent k = 17. Alice wants to transmit a secret number x. She calculates x^{17} (mod 91), sending the result 81 to Bob. Help Bob find x.

9. Mod 11:

$10 \ (mod\ 11)$ =

$100 \ (mod\ 11)$ =

$1000 \ (mod\ 11)$ =

$10^n \ (mod\ 11)$=

$19181716151413121110987654321 \ (mod\ 11)$ =

10. Perfect squares:

a) The sum of all the digits of a number A is 101. Prove that A cannot be a perfect square. (Hint: mod 3)

b) Consider the sequence: 11, 111, 1111, 11111, ... Prove that no element in this sequence can be a perfect square.
(Hint: mod 4)

11. Relation between working $mod\ n$ and working in $base\ n$:

$x\ mod\ n$ remembers only the last digit of the number x written in $base\ n$: