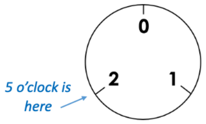
Modular Arithmetic

maths unboxed
www.youtube.com/mathsunboxed
www.instagram.com/maths_unboxed
mathsunboxed@gmail.com

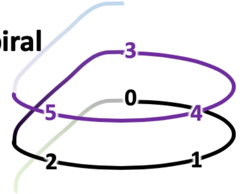
Introduction

Different ways to think about modular arithmetic: ***What is 5 (mod 3)?***

1. Clock



2. Spiral



3. Remainders

What is the remainder when I divide 5 by 3?

Answer = 2

4. Formal definition

5 minus what is divisible by 3?

Answer = 2

Formal definition: $x \equiv a \pmod{n}$ if $x - a$ is divisible by n *eg. $5 \equiv 2 \pmod{3}$ means that $5 - 2$ is divisible by 3*

Useful property: If $\mathbf{x \equiv a \pmod{n}}$ and $\mathbf{y \equiv b \pmod{n}}$ then: 1. $\mathbf{x + y \equiv a + b \pmod{n}}$ 2. $\mathbf{xy \equiv ab \pmod{n}}$

Proof of 1:

- ***SECRET AIM: Show that (x+y) – (a+b) is divisible by n (result then follows using the formal definition)***
- Have $x \equiv a \pmod{n}$ so $x - a$ is divisible by n *(using the formal definition).*
- That is, $\mathbf{x - a = kn}$ for some integer k.
- Similarly, $y \equiv b \pmod{n}$ so $y - b$ is divisible n and so $\mathbf{y - b = rn}$ for some integer r
- Then: $\mathbf{(x+y) - (a+b) = (x-a) + (y-b) = kn - rn = n(k-r)}$
- So $\mathbf{(x+y)-(a+b)}$ is divisible by $\mathbf{n}$, that is $\mathbf{x+y \equiv a+b \pmod{n}}$ as required ☺

Proof of 2:

Try this for yourself first by adapting the proof above! If you get stuck, the proof is at the bottom of the next page.

Examples of using Modular Arithmetic: *(There are video explanations to these on my YouTube channel)*

1. What is the final digit of 7^{100}?

- This is the same as asking "what is 7^{100} mod 10?". Have a think about why!
- Note that $7^{100} = \underbrace{7 \times 7 \times 7 \times \ldots \times 7}_{100\text{ times}}$. We want to use Useful Property 2 to help, but 7 is already reduced under modulo 10.
- However, we can group the 7's into pairs: $\underbrace{7 \times 7 \times 7 \times \ldots \times 7}_{100\text{ times}} = \underbrace{7^2 \times 7^2 \times \ldots \times 7^2}_{50\text{ times}} = \underbrace{49 \times 49 \times \ldots \times 49}_{50\text{ times}}$
- Normally we say that $49 \equiv 9 \pmod{10}$. But it's also true that $49 \equiv -1 \pmod{10}$ (make sure you see why)
- So we have that $7^{100} = \underbrace{49 \times 49 \times \ldots \times 49}_{50\text{ times}} \equiv \underbrace{(-1) \times (-1) \times \ldots \times (-1)}_{50\text{ times}} \pmod{10}$
- But an even product of -1's is just 1. So $7^{100} \equiv 1 \pmod{10}$ so the final digit of 7^{100} is 1.

2. Can 4003 be written as the <u>sum</u> of two <u>square</u> numbers?

- We prove it <u>can't</u> by using **proof by contradiction**. Suppose it can, say $4003 = x^2 + y^2$ where x and y are integers.
- Note that $4003 \equiv 3 \pmod{4}$. So we have that $x^2 + y^2 \equiv 3 \pmod{4}$. ❖
- x and y are each congruent to one of 0, 1, 2 or 3 (mod 4). *(every number is congruent to one of these mod 4).*
- So x^2 and y^2 are each congruent to one of $0^2, 1^2, 2^2, 3^2 \pmod{4}$.
- Note in mod 4: $0^2 = 0$, $1^2 = 1$, $2^2 = 4 \equiv 0$, $3^2 = 9 \equiv 1$. So x^2 and y^2 can each either be congruent to 0 or 1 (mod 4).
- So $x^2 + y^2$ <u>cannot</u> be congruent to 3 (mod 4) *(as no combination of two of 0's and 1's add to 3).*
- But this is a contradiction with ❖. Hence 4003 <u>cannot</u> be written as the sum of two square numbers.

More questions to try:

(you can check your answers to 1&2 using the website WolframAlpha)

1. What is 3^{99} mod 5?
2. What is the remainder when 2020^{2020} is divided by 3? *(note: this is the same as asking "what is 2020^{2020} (mod 3)?". Have a think about why!)*
3. Prove, using modular arithmetic, that there is no square number that is a multiple of 2 but not a multiple of 4. *(Hint: Use proof by contradiction. If there is such a number x, what is x (mod 4)? What values can square numbers take in modulo 4?)*

How to send secret messages using Modular Arithmetic *(the RSA algorithm)*

Say you are **Person A** and you want **Person B** to send you a top secret message that can't be decoded if it is intercepted by someone else.

A	B	C	D	E	F	G	H	I
1	2	3	4	5	6	7	8	9

Person A

1. Choose 2 distinct prime numbers **p**, **q** (each greater than 40 and less than 200)
2. Calculate **n** = **p** x **q**
3. Calculate **t** = (**p**-1)(**q**-1)
4. Choose a prime number **e** such that the highest common factor of **e** and **t** is 1.
5. On the website WolframAlpha search "What is the multiplicative inverse of **e** modulo **t**?". Call the result **d**. *(your search on WolframAlpha has found the multiplicative inverse of **e** (mod **t**) which is the number **d** such that **ed** ≡ **1** (mod **t**). Search up 'multiplicative inverses modular arithmetic' for more information on these numbers. If you're interested in how WolframAlpha calculates this, search up the 'Euclidean Algorithm'.*
6. **Give Person B the values of n and e** – in fact *everyone* can see this! Even the people who you don't want to read your future message can get these values; these values won't help them!

Person B

1. Choose a message that is 3 letters long using the letters A through to I. *(you can send longer messages if you send them in 3 letter chunks. You can also use different letters if you create a table assigning 9 letters of your choice the numbers 1-9.)*
2. Convert your message into numbers using the yellow table above. This is **M**. *Eg. If your message is 'CAB' then M = 312.*
3. Calculate M^e (mod **n**) using WolframAlpha *(type in the search bar "M^e (mod n)")*. Label this number **C**.
4. **Give C to Person A –** this is your encrypted message!

Person A

1. Compute C^d (mod **n**) using WolframAlpha. Convert this to letters using the table to receive the message!

*Note, that even if someone intercepted the message **C** when it passed from Person B to Person A, they would be unable to decrypt it as they don't have the value **d**, and they can't work it out from the values **n** and **e** (if they have these) due to how hard it is factor numbers if they are a product of two large primes.*

This is the method that most computers and large companies use to encrypt and decrypt information securely – except normally they choose **p** and **q** to be of over 1000 digits in length!

Further interesting things you can search up:

- Fermat's Little Theorem
- Multiplicative inverses in modular arithmetic
- Wilson's Theorem
- The Chinese Remainder Theorem

Proof of Useful Property 2:

- **SECRET AIM: Show that xy – ab is divisible by n**
- Have x ≡ a (mod n) so x - a = kn for some integer
- y ≡ b (mod n) so y - b = rn for some integer r
- Then: $xy - ab = (kn+a)(rn+b) - ab = (krn^2 + arn + bkn + ab) - ab = krn^2 + arn + bkn = n(krn + ar + bk)$
- So xy - ab is divisible by n, that is xy ≡ ab (mod n) as required *(using the formal definition)* ☺