Content of Course

- Prime and Hailstone sequences
- RSA encryption
- Chaotic Dynamical Systems.

Part I Primes and Hailstone Sequences.

~~Prime Numbers~~

- ~~A number that is divisible only by itself and one~~
- ~~A positive integer greater than 1 that is divisible only by itself and one.~~

~~Twin Primes~~

- ~~A pair of primes separated by 2~~
- ~~Eg. {3,5}, {17,19},~~

- Prime Number - A positive integer greater than 1 that is divisible by itself and one.
- Twin Prime - A pair of primes separated by 2.
  - Ex {3,5}, {17,19}.
- Theorem - There are infinitely many primes.
- Euclids Proof - Suppose that there are finitely many primes $(p_1, p_2, \dots p_n)$. Define $a = p_1, p_2, \dots p_n + 1$. 'a' is not in the list, thus 'a' is not a prime. Thus there is a p_i from the list that divides a. Now consider $a - p_1, p_2, \dots p_n = 1$, but p_i divides 'a' and $p_1, p_2, \dots p_n$; thus p_i divides $(a - p_1, p_2, \dots p_n)$ therefore p_i divides 1 (non-prime), Thus there are infinitely many primes. (by contradiction).

- Goldbach Conjecture - any even number (>2) can be written as the sum of two primes.
  - $4=2+2$, $6=3+3$, $12=5+7$,
  - $8=5+3$, $10=5+5$, $14=7+7$,
- Conjecture - no proof, no counter example.
- Fermat's Last Theorem - The equation $x^n+y^n=z^n$ has no solutions in positive integers for $n>2$.
- ~~Fermats Wyles Last~~ - $1^1+2^1=3^1$, $3^2+4^2=5^2$, $n\neq 3,4\ldots$
- Fermat's - Wyles Last Theorem - Wyles contributed the proof to fermats conjecture.
- How to check for prime number?
  - Divide said number by all of the primes leading up to it. (based on $>$)
- Fundamental Theorem of Arithmetics.
  - Any positive integer, $a>1$, can be written in a unique way as a product of primes.
  - $a=p_1^{e_1}\cdots p_k^{e_k}$, p_i = prime, e_i = positive integer
  - Ex. $12=2^2 3^1$
- Let $n=ab$, and claim that $a\leq\sqrt{n}$ or $b\leq\sqrt{n}$. If not (by way of contradiction) then $a>\sqrt{n}$ and $b>\sqrt{n}$. This means that $ab>\sqrt{n}\sqrt{n}>n \Rightarrow n>n$, nonsense. Therefore $a\leq\sqrt{n}$ or $b\leq\sqrt{n}$. Therefore it is sufficient to check divisions up to $\sqrt{n}$ to determine whether or not n is prime.

Hailstone Sequences

- Ex. 4, 2, 1; length=2
  Ex. 10, 5, 16, 8, 4, 2, 1; length=6
- Hailstone Sequence - ① take any positive integer, a
  ② if a is even, divide by 2 to get next term
  if a is odd, multiply by 3 and add 1 to get next
  ③ Repeat til 1 and stop.

Summary

- Number Theory ($\mathbb{Z}$)
  - specifically positive integers.
- Prime Numbers
  - twin primes
  - conjecture vs. theorem
  - proof & counter-example.
- Hailstone Sequences.
  - for n=6; 6, 3, 10, 5, 16, 8, 4, 2, 1.

Programming

Loops and Conditional Controls

- A. Loops ' Repetitive operations

```
For ( )
    ( Statements
Next.
```

- Ex1 -

```
Dim i, Count As Integer 'two variables are declared of type integers
Count = 0               'Value 0 is assigned to count.
For i = 1 to 3          ' 1 is assigned to count.
    Count = Count + 1   ' Vary with.
Next
TextBox1.Text = Count
```

- Eg 2

```
Dim i, Sum As Integer
For i = 1 to 3
    Sum += i        ' Sum = Sum + i
Next
TextBox1.Text = Sum.
```

- Eg 3

```
Dim i, Sum As Integer
For i = 1 to 3
    Sum += i
Next
Textbox1.Text = Sum
```

- Eg 4

```
Dim i, j As Integer
Dim Count As Long
Count = 0
For i = 1 to 2
    For j = 2 to 4
        Count += 1
    Next
Next.
Textbox1.Text = Count
```

Nested Loops.

- B- Conditional Controls
  - If (condition) then
    (statements)
    End If
  - OR If (condition) Then
    (statements)
    Else
    (statements)
    End If.

*Eg

```
Dim i, Count As Integer
i=5
Count=3
If i>4 Then
    Count *= 2
End If
Textbox1.Text = Count.
```

Lecture Goal

- Write a program that gives the length of a Hailstone Sequence
  - Reminder: The Collatz Conjecture - Let a_1 be a positive integer. Then the HS for which a_1 is the first term ends at 1 after finitely many steps.
- Eg take $a_1=10$, then the HS for 10 is

  $a_1=10$ $a_5=4$
  $a_2=5$ $a_6=2$
  $a_3=16$ $a_7=1$, length = 6.
  $a_4=8$
- Operation Mod.
  - mod n gives the remainder when m is divided by n.
  - $16 \bmod 5 = 1$.
    $23 \bmod 4 = 3$.
- Programming Tips:- Work incrementally.
  - code then test then code then test ...

a) Given a_n, display a_{n+1}

```
Dim x As Integer.
    X= Textbox1.Text.
If x Mod 2=0 Then
    Textbox2.Text = x/2.
Else
    Textbox2.Text = 3*x+1
End If
```

b) Given a_n, determine & display a_{n+1}

```
Dim x As Integer
    x = Textbox1.Text
If x Mod 2 = 0 Then
    x = x/2
Else
    x = 3*x+1
End If.
Textbox2.Text = x.
```

- c) Complete Code Idea

loop + repeat code (b).

loop until we reach 1 { code (b)

- Do While loops.
  - When we don't know how many times we have to repeat but we know "until a condition is satisfied"
  - Do While (condition)
    (statements)
    Loop.
  - Eg. Dim i As Integer
    i = 1.
    Do while i < 5
    i += 2.
    Loop
    Textbox2.Text = i

i	i
1	1, 3, 5.

Avoid infinite loops.

- c) Complete Code Idea.

```
Dim seed As Integer
Seed = Textbox1.Text
Do While Seed > 1
    If Seed Mod 2 = 0 Then
        Seed = Seed / 2
    Else
        Seed = 3 * Seed + 1
    End If
Loop
TextBox2.Text = Seed.
```

Integer → Long. for longer numbers.

```
Dim Seed, Length As Integer
Seed = Textbox1.Text
Length = 0
Do while Seed > 1
    If Seed Mod 2 = 0 Then
        Seed = Seed / 2.
    Else
        Seed = 3 * Seed + 1
    End If.
    Length = Length + 1.
Loop.
Textbox2.Text = Length.
```

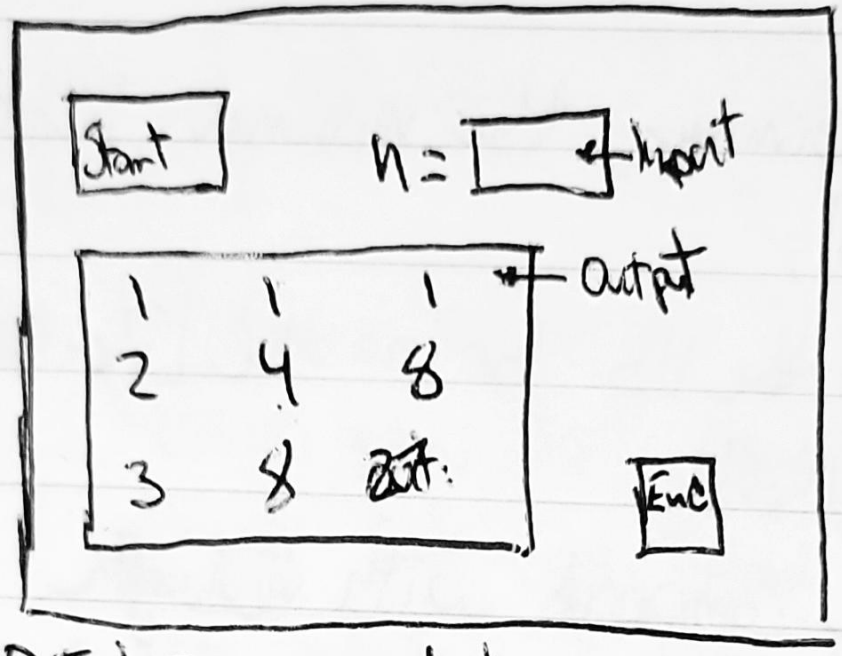
Lecture Goal

- To create a program to determine the maximum length of a Hailstone for $n \leq 10,001$.
- Needs: - code of length of the HS for n = seed [Recursive (last weekend) code]
  - for seed = 1 to 10,001.
  - maxlength to be compared with newlength
- Code:

```
Dim Seed, i, Length, Upperbound, Maxlength, Maxseed As Long
Upperbound = Textbox1.Text   'eg. 10001
Max length = 0
Maxseed = 1.
For i = 1 To Upperbound
    Length = 0
    Seed = i
    Do While Seed > 1
        If Seed Mod 2 = 0 Then
            Seed = Seed / 2
        Else
            Seed = 3 * Seed + 1
        End If
        Length = length + 1
    Loop
    If Length > Maxlength Then
        Maxlength = length
        Maxseed = i
    End If
Next.
Textbox2.Text = Maxlength
Textbox3.Text = Maxseed
```

Interface to Show Many Output in a Table

- Eg.



- ~~Text~~ Output Box → Multiline = True.
  Scroll bar = Vertical.

Part II RSA Encryption

- RSA → Rivest-Shamir-Adleman (1977).
- Have to make an unbreakable code that anyone can encode but only one person can decode ("trap door cipher")
- Algebra Background
  - What is the remainder of 18/5?
    - $18 \bmod 5 = 3$
  - take $x = 23$, $y = 1004$.
    - $x \bmod 5 = 3$
      $y \bmod 5 = 4$
  - $x + y = 23 + 1004$
    $= 1027 \rightarrow 1027 \bmod 5 = 2$.
  - $xy = (23)(1004)$.
    $= 23092 \rightarrow 23092 \bmod 5 = 2$

  $x \bmod 5 + y \bmod 5 = 3 + 4$
  $= 7 \rightarrow 7 \bmod 5 = 2$.
  $(x \bmod 5)(y \bmod 5) = 12$
  $= 12 \rightarrow 12 \bmod 5 = 2$.

- mod 5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

- Arithmetic in the integers modulus 5"
  - $\mathbb{Z}_5 = \{0,1,2,3,4\}$, together with +, ·
- Define - $\mathbb{Z}_n = \{0,1,2,\ldots n-1\}$, together with +, ·
- "Clock" Arithmetic

$\mathbb{Z}_6$ ① $4+3 \bmod 6 = 1$
② $4 \cdot 3 \bmod 6 = 0$

- $\mathbb{Z}_6$

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$xy = n6$ For prime, no small integer factor → no zeros.

* Inverse Element - find where the remainder is 1.

- $\mathbb{Z}_5$

0	none
1	1
2	3
3	2
4	4

$\mathbb{Z}_6$

0	none
1	1
2	none
3	none
4	none
5	5

* $\mathbb{Z}_6$ - integers mod 6.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

- $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$; together +, ·; the set of all remainders when divided by 6.
- "Clock arithmetic."
- 26 mod 6 = 2.
- 5·5 mod 6 = 1., thus 5 is the inverse of itself.

* ← Lets look at all the inverse in $\mathbb{Z}_7$.

- $\mathbb{Z}_7$

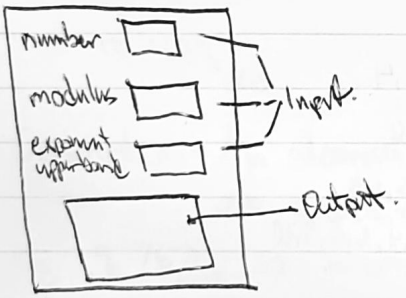
	inverses
0	none
1	1
2	4
3	5
4	2
5	3
6	6

* Observation - Similar to $\mathbb{Z}_5$, every non-zero element in $\mathbb{Z}_7$ has an inverse.
* Definition - We say that a is congruent to b modulo n, denoted by $a \equiv b \bmod n$, provided that a & b have the same remainder after divided by n.

- Note: this is equivalent to say when $n \mid (b-a)$,
  "n divides evenly into (b-a)"
  ↳ no remainder for $\frac{b-a}{n}$.

- Eg① $6 \equiv 8 \bmod 2$.
  Since $2 \mid (8-6)$
  OR
  since 6 has a remainder of 0 when divided by 2 and so does 8.
- Eg② $6 \not\equiv 8 \bmod 3$
  Since $3 \nmid (8-6)$
  2.
- Eg③ $24 \equiv 39 \bmod 5$
  Since $5 \mid (39-24)$
- Eg④ $2^8 \equiv 1 \bmod 5$.
  $(2^4)^2 \equiv 1 \bmod 5$.
  $16 \equiv 1 \bmod 5$ ✓, $\Rightarrow 2^4 \equiv 1 \bmod 8$.
- Eg⑤ $2^{1002} \equiv ? \bmod 5$.
  $(2^4)^{250} \cdot 2^2 \equiv (1)^{250} \cdot 2^2 \bmod 5$.
  thus $2^{1002} \equiv 4 \bmod 5$.

-



- Idea - $3^0 = 1$ "power" → power = 1
  $3^1 \mid 1 \cdot 3 = 3$
  $3^2 \mid 3 \cdot 3 \equiv 4 \bmod 5$
  $3^3 \mid 4 \cdot 3 = 2 \bmod 5$.
  For i = 1 to upperbound
  → power = power * number Mod 5.
  adding the table for output → Next

- Theorem - If $a \equiv b \bmod n$ and $c \equiv d \bmod n$ then $(a+c) \equiv (b+d) \bmod n$.
  Proof - we want to show that $n \mid (b+d)-(a+c)$, but $(b+d)-(a+c) = (b-a)+(d-c)$
  thus $n \mid (b-a)+(d-c)$

- Theorem - If $a \equiv b \bmod n$, and if $c \equiv d \bmod n$ then
  $a \cdot b \equiv b \cdot d \bmod n$
- Proof - Idea similar to previous proof
  $n \mid (a-b) \Rightarrow n \mid (a-b) \cdot c$
  $n \mid (c-d) \Rightarrow n \mid (c-d) \cdot b$
  Thus ..... (exercise).
- What do these theorems tell us?
  - A result (in addition & multiplication) that holds in $\mathbb{Z}$ is also true in any $\mathbb{Z}_n$
  - Exercise generate 2 examples for each theorem.
- Definition. An element $a \in \mathbb{Z}_n$ is called invertible in $\mathbb{Z}_n$ if there is an element $b \in \mathbb{Z}$ such that $ab \equiv 1 \bmod n$.
- Eg. 2 is invertible in $\mathbb{Z}_5$. Since $2 \cdot 3 \equiv 1 \bmod 5$ but 2 is not invertible in $\mathbb{Z}_6$ since $2 \cdot 0 \ldots 5 \equiv 1 \bmod 6$.
- We are interested in finding out invertible elements in $\mathbb{Z}_n$. Next class.

$\mathbb{Z}_n$	Invertible Element	Non-Invertible Element
2	1	0
3	1,2	0
4	1,3	0,2
5	1,2,3,4	0
6	1,5	0,2,3,4
7	1,2,3,4,5,6	0
8	1,3,5,7	0,2,4,6
9	1,2,4,5,7,8	0,3,6,
10	1,3,7,9	0,2,4,5,6,9
11	1,2,3,4,5,6,7,8,9,10,11	0
12	1,5,7,11	0,2,3,4,6,8,9,10

- Observations
  - ① Every non-zero element in $\mathbb{Z}_p$ (p=prime) is invertible (theorem).
  - ② 0 is always non-invertible & 1 is always invertible in any $\mathbb{Z}_n$ $n \geq 2$
  - ③ $n-1$ is always invertible in $\mathbb{Z}_n$
  - ④ Invertible elements in $\mathbb{Z}_n$ never share prime factors with n.

- Definition - Two integers a & b are coprime or relatively prime if there are no common prime factors.
  - Note: This is equivalent to say that their greatest common divisor is 1, hence $\gcd(a,b)=1$.
- Eg. $\gcd(16,10)=2$.
  $\gcd(11,52)=1$, are relatively prime (tells us 11 is invertible in $\mathbb{Z}_{52}$)
  $\gcd(24,10)=2$,
- How can one find the gcd of any two numbers?
  - Algorithm (Euclid)
  - $24 = n10 + i$
    $= 2(10) + 4$.
    $10 = n4 + i$
    $= (2)4 + 2$
    $4 = n2 + i$
    $4 = 2(2) + 0$
    This is our gcd
- $\gcd(52,64) = 4$.
  $62 = n52 + i$
  $62 = (1)52 + 12$
  $52 = (4)12 + 4$
  $12 = (3)4$
  gcd
- Observation: An element $a \in \mathbb{Z}_n$ is invertible $\Leftrightarrow \gcd(a,n)=1$
- Eg $76 \in \mathbb{Z}_{20}$ is invertible since $\gcd(7,20)=1$. Indeed $7 \cdot 3 \equiv 1 \bmod 20$
  $7 \in \mathbb{Z}_{35}$ is not invertible since $\gcd(7,35)=7 \neq 1$. 7 & 35 are not relatively prime.

The Euler φ Function

- Define: $\varphi(n)$ is the number of positive integers smaller than n that are relatively prime to n
- Eg. $\varphi(3)=2$: $1, 2$
  $\varphi(4)=2$: $1, 2, 3$
  $\varphi(5)=4$: $1, 2, 3, 4$
  $\varphi(6)=2$: $1, 2, 3, 4, 5$
- Note: $\varphi(n)$ gives the number of invertible elements in $\mathbb{Z}_n$
- We will want to calculate $\varphi(n)$ for large n
- Question: if $ab=n$ then $\varphi(a)\varphi(b)=\varphi(n)$?
  Is φ multiplicative?

$\varphi(7)=6$: $1, 2, 3, 4, 5, 6$

- We Explore:

a	b	ab	φ(a)	φ(b)	φ(ab)	Multiplicative?
3	3	9	2	2	6	No
7	2	14	6	1	6	Yes
4	2	8	2	1	4	No
4	4	16	2	2	8	No
4	5	20	2	4	8	Yes
2	10	20	1	4	8	No

Review:
$\mathbb{Z}_n$, $+$, $\cdot$ "Mod" in Visual
$a \equiv b \bmod n$
Eg. 7^5 in $\mathbb{Z}_{12}$.
Inverses in $\mathbb{Z}$.
Eg 7 is invertible in $\mathbb{Z}_{10}$
Since $\gcd(7,10)=1$
The number of elements in $\mathbb{Z}_n$ is given by $\varphi(n)$
$\varphi(p)=p-1$ ← prime.

- Theorem: If a & b are relatively prime, then $\varphi(ab)=\varphi(a)\varphi(b)$
- Corollary: If p & q are two distinct primes, then
  $\varphi(pq)=(p-1)(q-1)$
  - Proof: $\varphi(p,q)=\varphi(p)\varphi(q)$ since $\gcd(pq)=1$
    $=(p-1)(q-1)$ since p & q are prime.
- Euler's Theorem - If $\gcd(a,n)=1$, $a^{\varphi(n)} \equiv 1 \bmod n$.
  - Eg $a=2, m=3$
    $\gcd(2,3)=1$, $\varphi(3)=2$, $2^2=4$.
    $2^{\varphi(3)} \equiv 1 \bmod 3 \equiv 4 \equiv 1 \bmod 3$
  - Eg $a=3$, $n=1,000,000,007$
    $\gcd(a,n)=1$, $3^{\varphi(n)}=3^{1000000006}$
    $3^{1000000007} \equiv 1 \bmod 1000000007$

RSA Encryption

- Rivest - Shamir - Adleman
- Alice <--message--> Bob a method so that everyone knows how to encode messages to Alice but only A knows how to decode it. "Trapdoor cypher"
- It is based on the fact that it is virtually impossible to factor very large numbers $> 10^{200}$
- Here is the procedure
- Part 1: Alice prepares her public key
  1) Alice selects two distinct giant prime numbers $> 10^{100}$
     Eg. $p=23$, $q=41$
  2) Find $n=pq$, $\varphi(n)=\varphi(pq)$
     Eg. $n=pq=943$
     $\varphi(n)=(p-1)(q-1)=880$
  3) Alice chooses a number 'e' relatively prime to $\varphi(n)$
     Eg. Alice selects $e=7$ where by $\gcd(7,880)=1$ and Alice publishes the public key: (n,e) & everyone can see the public key.
     Eg Alice publishes $(943,7)$.
- Part 2: Bob sends encrypted secret message to Alice.
  4) Assume the message is turned into numbers (ref: labs)
     Eg. $M=35$
  5) Bob encrypts message by calculation $M^e \bmod n = c$
     c = "coded message"
     Eg $35^7 \bmod 943 = 545$
     Bob sends $C=545$ to Alice and everyone can see it.
- Part 3: Back to Alice to decode the message recieved
  6) Alice calculates the "private key" by finding d such that $e \cdot d \equiv 1 \bmod \varphi(n)$
     Eg. Alice find d such that
     $7d \equiv 1 \bmod 880$
     $d=503$ (and keeps) secret
  7) Alice decodes message by calculating $c^d \bmod n = M$ Eg. $545^{503} \bmod 943 = 35$.