



Spring 2021 - March 11, 2021

## Caesar Encryption

## Exercise – Caesar Encryption

#### Write a program that

- runs through a given string
- $\blacksquare$  decrypts each letter with a key k
- $\blacksquare$  tries out each key k
- uses the following formula

$$e = (v - 65 - k) \% 26 + 65$$



Decrypt the ciphertext

TYQZCXLETVTDEVCPLETGPLCMPTE

## Exercise – Caesar Encryption

```
for k in range(0, 26):
   for item in ciphertext:
      print(chr((ord(item) - 65 - k) % 26 + 65), end="")
   print()
```

```
for k in range(0, 26):
   for i in range(0, len(ciphertext)):
      print(chr((ord(ciphertext[i]) - 65 - k) % 26 + 65), end="")
   print()
```

# Changing the Step Size

## Loops over Lists – Larger Steps

Traverse a list with steps of length 2

## Loops over Lists – Larger Steps

#### Traverse a list with steps of length 2

```
data = [5, 1, 4, 3]
for i in range(0, len(data), 2):
    print(data[i])
```

## Loops over Lists – Larger Steps

#### Traverse a list with steps of length 2

```
data = [5, 1, 4, 3]
for i in range(0, len(data), 2):
    print(data[i])
```

#### Output

All elements at even positions from 0 up to at most len(data) are output  $\Rightarrow$  5.4

for i in range(start, end, step)

for i in range(start, end, step)

Iteration over all positions from start up to end-1 with step length of step

```
for i in range(start, end, step)
```

Iteration over all positions from start up to end-1 with step length of step

#### Shorthand notation

```
for i in range(start,end) \iff for i in range(start,end,1)
```

```
for i in range(start, end, step)
```

Iteration over all positions from start up to end-1 with step length of step

#### Shorthand notation

```
for i in range(start,end) \iff for i in range(start,end,1)
```

#### Another shorthand notation

```
for i in range(end) \iff for i in range(0, end)
```

## Improvement of Caesar Encryption

Use two keys alternatingly for even and odd positions

## Improvement of Caesar Encryption

#### Use two keys alternatingly for even and odd positions

```
k = int(input("First key: "))
l = int(input("Second key: "))
x = input("Text (only uppercase, even length): ")
for i in range(0, len(x), 2):
    print(chr((ord(text[i]) - 65 + k) % 26 + 65), end="")
    print(chr((ord(text[i+1]) - 65 + 1) % 26 + 65), end="")
print()
```

## Improvement of Caesar Encryption

#### Use two keys alternatingly for even and odd positions

```
k = int(input("First key: "))
l = int(input("Second key: "))
x = input("Text (only uppercase, even length): ")
for i in range(0, len(x), 2):
    print(chr((ord(text[i]) - 65 + k) % 26 + 65), end="")
    print(chr((ord(text[i+1]) - 65 + 1) % 26 + 65), end="")
print()
```

#### Still Caesar encryption remains insecure □ Project 1

## Logical Values

**Boolean Values and Relational Operators** 

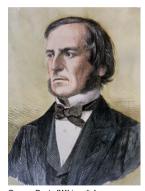
Boolean expressions can take on one of two values F or T

#### Boolean expressions can take on one of two values F or T

- F corresponds to "false"
- T corresponds to "true"

#### Boolean expressions can take on one of two values F or T

- F corresponds to "false"
- T corresponds to "true"



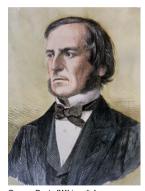
George Boole [Wikimedia]

#### Boolean expressions can take on one of two values F or T

- F corresponds to "false"
- T corresponds to "true"

#### **Boolean variables in Python**

- represent "logical values"
- Domain {False, True}



George Boole [Wikimedia]

#### Boolean expressions can take on one of two values F or T

- F corresponds to "false"
- T corresponds to "true"

#### **Boolean variables in Python**

- represent "logical values"
- Domain {False, True}

#### Example

b = True # Variable with value True



George Boole [Wikimedia]

$$x < y$$
 (smaller than)

 $number\ type \times number\ type \rightarrow \{\texttt{False,\ True}\}$ 

$$x < y$$
 (smaller than)

$$b = (1 < 3)$$

$$x < y$$
 (smaller than)

$$b = (1 < 3)$$
 #  $b = True$ 

$$x \ge y$$
 (greater than)

$$x = 0$$
  
 $b = (x >= 3)$  #  $b =$ 

$$x \ge y$$
 (greater than)

$$x = 0$$
  
b = (x >= 3) # b = False

$$x == y$$
 (equals)

$$x = 4$$
  
b = (x % 3 == 1) # b =

$$x == y$$
 (equals)

$$x != y$$
 (unequal to)

$$x = 1$$
  
 $b = (x != 2 * x - 1) # b =$ 

$$x != y$$
 (unequal to)

$$x = 1$$
  
b =  $(x != 2 * x - 1) # b = False$ 

## Logical Values

**Boolean Functions and Logical Operators** 

### **Boolean Functions in Mathematics**

#### **Boolean function**

$$f: \{\mathbf{F}, \mathbf{T}\}^2 \to \{\mathbf{F}, \mathbf{T}\}$$

- F corresponds to "false"
- T corresponds to "true"

#### $\overline{a} \wedge \overline{b}$

#### "logical and"

$$f \colon \{\mathbf{F}, \mathbf{T}\}^2 \to \{\mathbf{F}, \mathbf{T}\}$$

- F corresponds to "false"
- T corresponds to "true"

a	b	$a \wedge b$
F	F	F
F	Т	F
Т	F	F
Т	Т	Т

## Logical Operator and

a and b (logical and)

 $\{\texttt{False, True}\} \times \{\texttt{False, True}\} \rightarrow \{\texttt{False, True}\}$ 

## Logical Operator and

```
n = -1

p = 3

c = (n < 0) and (0 < p) # c =
```

## Logical Operator and

```
n = -1

p = 3

c = (n < 0) and (0 < p) # c = True
```

#### $a \vee b$

"logical or"

$$f: \{\mathsf{F},\mathsf{T}\}^2 \to \{\mathsf{F},\mathsf{T}\}$$

- F corresponds to "false"
- T corresponds to "true"

a	b	$a \lor b$
F	F	F
F	Т	Т
Т	F	Т
т	Т	Т

#### $a \vee b$

"logical or"

$$f: \{\mathsf{F},\mathsf{T}\}^2 \to \{\mathsf{F},\mathsf{T}\}$$

- F corresponds to "false"
- T corresponds to "true"

a	b	$a \lor b$
F	F	F
F	Т	Т
т	F	Т
Т	Т	Т

The **logical or** is always **inclusive**: a or b or both

## Logical Operator or

 $\{False, True\} \times \{False, True\} \rightarrow \{False, True\}$ 

## Logical Operator or

$$n = 1$$
  
 $p = 0$   
 $c = (n < 0) \text{ or } (0 < p)$  #  $c =$ 

### Logical Operator or

```
n = 1
p = 0
c = (n < 0) or (0 < p) # c = False</pre>
```

"logical not"

$$f \colon \{\mathsf{F},\mathsf{T}\} \to \{\mathsf{F},\mathsf{T}\}$$

- F corresponds to "false"
- T corresponds to "true"

b	$\neg b$
F	Т
Т	F

## Logical Operator not

not b (logical not)

 $\{\texttt{False, True}\} \rightarrow \{\texttt{False, True}\}$ 

## Logical Operator not

$$n = 1$$
 $a = not (n < 0) # a =$ 

## Logical Operator not

## **Logical Values**

not b and a

a and b or c and d

a or b and c or d

$$b = 7 + x < y \text{ and } y != 3 * z \text{ or not } b$$

$$b = 7 + x < y \text{ and } y != 3 * z \text{ or not } b$$
  
 $b = (7 + x) < y \text{ and } y != (3 * z) \text{ or not } b$ 

■ Binary arithmetic operators bind the strongest (multiplication and division first, then addition and subtraction)

$$b = 7 + x < y \text{ and } y != 3 * z \text{ or not } b$$
  
 $b = ((7 + x) < y) \text{ and } (y != (3 * z)) \text{ or not } b$ 

- Binary arithmetic operators bind the strongest (multiplication and division first, then addition and subtraction)
- These bind stronger than **relational operators** (and first, then or)

$$b = 7 + x < y \text{ and } y != 3 * z \text{ or not } b$$
  
 $b = ((7 + x) < y) \text{ and } (y != (3 * z)) \text{ or (not b)}$ 

- Binary arithmetic operators bind the strongest (multiplication and division first, then addition and subtraction)
- These bind stronger than **relational operators** (and first, then or)
- These bind stronger than the unary logical operator not

```
b = 7 + x < y \text{ and } y != 3 * z \text{ or not } b

b = (((7 + x) < y) \text{ and } (y != (3 * z))) \text{ or (not b)}
```

- Binary arithmetic operators bind the strongest (multiplication and division first, then addition and subtraction)
- These bind stronger than **relational operators** (and first, then or)
- These bind stronger than the unary logical operator not
- These bind stronger than **binary logical** operators (and first, then or)

```
b = 7 + x < y \text{ and } y != 3 * z \text{ or not } b

b = ((((7 + x) < y) \text{ and } (y != (3 * z))) \text{ or (not } b))
```

- Binary arithmetic operators bind the strongest (multiplication and division first, then addition and subtraction)
- These bind stronger than **relational operators** (and first, then or)
- These bind stronger than the unary logical operator not
- These bind stronger than **binary logical** operators (and first, then or)
- These bind stronger than the assignment operator

$$b = 7 + x < y \text{ and } y != 3 * z \text{ or not } b$$

- Binary arithmetic operators bind the strongest (multiplication and division first, then addition and subtraction)
- These bind stronger than **relational operators** (and first, then or)
- These bind stronger than the unary logical operator not
- These bind stronger than **binary logical** operators (and first, then or)
- These bind stronger than the assignment operator
- It is often useful to use parentheses even if redundant

## DeMorgan Rules

## DeMorgan Rules

```
■ not (a and b) == (not a or not b)
```

## DeMorgan Rules

- not (a and b) == (not a or not b)
- not (a or b) == (not a and not b)

#### Examples

- (not black and not white) == not (black or white)
- not (rich and beautiful) == (poor or ugly)

(a or b) and not (a and b)

(a or b) and not (a and b)

a or b, and not both

(a or b) and not (a and b)

a or b, and not both

(a or b) and (not a or not b)

(a or b) and not (a and b)

a or b, and not both

(a or b) and (not a or not b)

a or b, and one of them not

(a or b) and not (a and b)

a or b, and not both

(a or b) and (not a or not b)

a or b, and one of them not

not (not a and not b) and not (a and b)

(a or b) and not (a and b)

a or b. and not both

(a or b) and (not a or not b)

a or b. and one of them not

not (not a and not b) and not (a and b) not none and not both

```
(a or b) and not (a and b)
                                            a or b. and not both
(a or b) and (not a or not b)
                                            a or b. and one of them not
not (not a and not b) and not (a and b) not none and not both
not ((not a and not b) or (a and b))
```

```
(a or b) and not (a and b)
                                            a or b. and not both
                                             a or b. and one of them not
(a or b) and (not a or not b)
not (not a and not b) and not (a and b) not none and not both
not ((not a and not b) or (a and b))
                                             not: both or none
```

# Control Structures

#### **Control Flow**

So far...

■ Up to now linear (from top to bottom)

### Control Flow

#### So far...

- Up to now linear (from top to bottom)
- for loop to repeat blocks

```
x = int(input("Input: "))
for i in range(1, x+1):
    print(i*i)
```

# **Control Structures**

**Selection Statements** 

#### Selection Statements

#### Implement branches

- if statement
- if-else statement
- if-elif-else statement (later)

if condition: statement

```
if condition: statement
```

```
x = int(input("Input: "))
if x % 2 == 0:
    print("even")
```

if condition: statement

If *condition* is true, then *statement* is executed

```
x = int(input("Input: "))
if x % 2 == 0:
    print("even")
```

# if condition: statement

```
x = int(input("Input: "))
if x % 2 == 0:
    print("even")
```

If *condition* is true, then *statement* is executed

- statement:
  - arbitrary statement
  - **body** of the **if**-Statement
- condition: Boolean expression

if condition:
 statement1
else:
 statement2

```
if condition:
    statement1
else:
    statement2
```

```
x = int(input("Input: "))
if x % 2 == 0:
    print("even")
else:
    print("odd")
```

```
if condition:
    statement1
else:
    statement2
```

```
x = int(input("Input: "))
if x % 2 == 0:
    print("even")
else:
    print("odd")
```

If condition is true, then statement1 is executed, otherwise statement2 is executed

```
if condition:
    statement1
else:
    statement2
```

```
x = int(input("Input: "))
if x % 2 == 0:
    print("even")
else:
    print("odd")
```

If condition is true, then statement1 is executed, otherwise statement2 is executed

- condition: Boolean expression
- statement1:
  body of the if-branch
- statement2: body of the else-branch

### Layout

```
x = int(input("Input: "))

if x % 2 == 0:
    print("even")

else:
    print("odd")
```

### Layout

Attention when using == or =

#### Attention when using == or =

An attempt to make a change in this way is suspicious, to say the least, so there was a lot of interest in what the attempted change was. The actual patch confirmed all suspicious; the relevant code was:

```
+ if ((options == (_WCLONE|_WALL)) && (current->uid = 0))
+ retval = -EINVAL;
```

It looks much like a standard error check, until you notice that the code is not testing current->uid - it is, instead setting it to zero. A program which called wait4() with the given flags set would, thereafter, be running as root. This is, in other words, a classic back door.

The resulting vulnerability, had it ever made it to a deployed system, would have been a locally-exploitable hole. Some sites have said that the hole would have been susceptible to remote exploits, but that is not the case. An attacker would need to be able to run a program on the target system first.

## **Control Structures**

while condition: statement

- statement:
  - arbitrary statement
  - body of the while loop
- condition: Boolean expression

```
while condition:

statement ← Indentation
```

- statement:
  - arbitrary statement
  - body of the while loop
- condition: Boolean expression

while condition: statement



■ True: iteration starts

statement is executed ■

■ False: while loop ends

```
s = 0
i = 1
while i <= 2:
    s = s + i
    i = i + 1</pre>
```

i condition s

```
s = 0
i = 1
while i <= 2:
    s = s + i
    i = i + 1</pre>
```

condition	s
	condition

```
s = 0
i = 1
while i <= 2:
    s = s + i
    i = i + 1</pre>
```

i	condition	s
i = 1	i <= 2?	

```
s = 0
i = 1
while i <= 2:
    s = s + i
    i = i + 1</pre>
```

i	condition	s
i = 1	true	

```
s = 0
i = 1
while i <= 2:
    s = s + i
    i = i + 1</pre>
```

i	condition	s
i = 1	true	s = 1

i	condition	s
i = 1 i = 2	true	s = 1

```
s = 0
i = 1
while i <= 2:
    s = s + i
    i = i + 1</pre>
```

i	condition	s
i = 1 i = 2	true i <= 2?	s = 1

```
s = 0
i = 1
while i <= 2:
    s = s + i
    i = i + 1</pre>
```

i	condition	s
i = 1	true	s = 1
i = 2	true	

```
s = 0
i = 1
while i <= 2:
    s = s + i
    i = i + 1</pre>
```

i	condition	s
i = 1	true	s = 1
i = 2	true	s = 3

```
s = 0
i = 1
while i <= 2:
    s = s + i
    i = i + 1</pre>
```

i	condition	ន
i = 1	true	s = 1
i = 2	true	s = 3
i = 3		

```
s = 0
i = 1
while i <= 2:
    s = s + i
    i = i + 1</pre>
```

i	condition	s
i = 1	true	s = 1
i = 2	true	s = 3
i = 3	i <= 2?	

```
s = 0
i = 1
while i <= 2:
    s = s + i
    i = i + 1</pre>
```

i	condition	s
i = 1	true	s = 1
i = 2	true	s = 3
i = 3	false	

```
s = 0
i = 1
while i <= 2:
    s = s + i
    i = i + 1</pre>
```

i	condition	ន
i = 1	true	s = 1
i = 2	true	s = 3
i = 3	false	s = 3

Use simplified syntax for changing values of variables

#### Use simplified syntax for changing values of variables

 $\mathbf{n}$   $\mathbf{n}$  =  $\mathbf{n}$  + 1 is written as  $\mathbf{n}$  += 1

#### Use simplified syntax for changing values of variables

- $\mathbf{n}$   $\mathbf{n}$  =  $\mathbf{n}$  + 1 is written as  $\mathbf{n}$  += 1
- $\mathbf{n}$   $\mathbf{n}$   $\mathbf{n}$   $\mathbf{n}$  +  $\mathbf{i}$  is written as  $\mathbf{n}$  +=  $\mathbf{i}$

#### Use simplified syntax for changing values of variables

- $\mathbf{n}$   $\mathbf{n}$  =  $\mathbf{n}$  + 1 is written as  $\mathbf{n}$  += 1
- $\mathbf{n}$   $\mathbf{n}$   $\mathbf{n}$   $\mathbf{n}$  +  $\mathbf{i}$  is written as  $\mathbf{n}$  +=  $\mathbf{i}$
- $\mathbf{n} = \mathbf{n} 15$  is written as  $\mathbf{n} = 15$

## Incrementation of Variables

#### Use simplified syntax for changing values of variables

- $\mathbf{n}$   $\mathbf{n}$  =  $\mathbf{n}$  + 1 is written as  $\mathbf{n}$  += 1
- $\mathbf{n}$   $\mathbf{n}$  =  $\mathbf{n}$  +  $\mathbf{i}$  is written as  $\mathbf{n}$  +=  $\mathbf{i}$
- $\mathbf{n} = \mathbf{n} 15$  is written as  $\mathbf{n} = 15$
- $\mathbf{n} = \mathbf{n} * \mathbf{j}$  is written as  $\mathbf{n} *= \mathbf{j}$

## Incrementation of Variables

#### Use simplified syntax for changing values of variables

- $\mathbf{n}$   $\mathbf{n}$  =  $\mathbf{n}$  + 1 is written as  $\mathbf{n}$  += 1
- $\mathbf{n}$   $\mathbf{n}$  =  $\mathbf{n}$  +  $\mathbf{i}$  is written as  $\mathbf{n}$  +=  $\mathbf{i}$
- n = n 15 is written as n -= 15
- $\mathbf{n} = \mathbf{n} * \mathbf{j}$  is written as  $\mathbf{n} *= \mathbf{j}$
- $\mathbf{n}$   $\mathbf{n}$   $\mathbf{n}$   $\mathbf{n}$  \*\* 4 is written as  $\mathbf{n}$  \*\*= 4

## Incrementation of Variables

## Use simplified syntax for changing values of variables

- $\mathbf{n} = \mathbf{n} + 1$  is written as  $\mathbf{n} += 1$
- $\mathbf{n}$   $\mathbf{n}$  =  $\mathbf{n}$  +  $\mathbf{i}$  is written as  $\mathbf{n}$  +=  $\mathbf{i}$
- n = n 15 is written as n -= 15
- $\mathbf{n} = \mathbf{n} * \mathbf{j}$  is written as  $\mathbf{n} *= \mathbf{j}$
- $\mathbf{n}$   $\mathbf{n}$   $\mathbf{n}$   $\mathbf{n}$  \*\* 4 is written as  $\mathbf{n}$  \*\*= 4
- . . . .

## The Jump Statements break

#### break

- Immediately leave the enclosing loop
- Useful in order to be able to break a loop "in the middle"

## The Jump Statements break

#### break

- Immediately leave the enclosing loop
- Useful in order to be able to break a loop "in the middle"

```
s = 0
while True:
    x = int(input("Enter a positive number, abort with 0: "))
    if x == 0:
        break
    s += x
print(s)
```

# **Control Structures**

**Termination** 

illioi Structures

```
i = 1
while i <= n:
    s += i
    i += 1</pre>
```

```
i = 1
while i <= n:
    s += i
    i += 1</pre>
```

#### Here and commonly

■ statement changes its value that appears in condition

```
i = 1
while i <= n:
    s += i
    i += 1</pre>
```

#### Here and commonly

- statement changes its value that appears in condition
- After a finite number of iterations condition becomes false

```
i = 1
while i <= n:
    s += i
    i += 1</pre>
```

#### Here and commonly

- statement changes its value that appears in condition
- After a finite number of iterations condition becomes false
- **⇒** Termination

## Infinite Loops

Infinite loops are easy to generate

```
while True:
    print("0")

while not False:
    print("1")

while 2 > 1:
    print("2")
```

## Infinite Loops

Infinite loops are easy to generate

```
while True:
    print("0")

while not False:
    print("1")

while 2 > 1:
    print("2")
```

■ ... but can in general not be automatically detected

## Halting Problem

## Undecidability of the Halting Problem [Alan Turing, 1936]

- There is no Python program that can determine, for each Python program *P* and each input *I*, whether *P* terminates with the input *I*
- This means that the termination of programs can in general not be automatically checked

## Halting Problem

## Undecidability of the Halting Problem [Alan Turing, 1936]

- There is no Python program that can determine, for each Python program *P* and each input *I*, whether *P* terminates with the input *I*
- This means that the termination of programs can in general not be automatically checked



Alan Turing [Wikimedia]

Theoretical questions of this kind were the main motivation for Turing to design his computing machine

Sequence of natural numbers  $n_0, n_1, n_2, n_3, n_4, n_5, \dots$ 

Sequence of natural numbers  $n_0, n_1, n_2, n_3, n_4, n_5, \dots$ 

$$\blacksquare$$
  $n_0 = n$ 

$$\blacksquare \text{ for every } i \geq 1, n_i = \begin{cases} n_{i-1}/2 & \text{if } n_{i-1} \text{ even} \\ 3 \cdot n_{i-1} + 1 & \text{if } n_{i-1} \text{ odd} \end{cases}$$

Sequence of natural numbers  $n_0, n_1, n_2, n_3, n_4, n_5, \dots$ 

$$\blacksquare$$
  $n_0 = n$ 

$$\blacksquare \text{ for every } i \geq 1, n_i = \begin{cases} n_{i-1}/2 & \text{if } n_{i-1} \text{ even} \\ 3 \cdot n_{i-1} + 1 & \text{if } n_{i-1} \text{ odd} \end{cases}$$

Example for n=5

## Sequence of natural numbers $n_0, n_1, n_2, n_3, n_4, n_5, \dots$

$$\blacksquare$$
  $n_0 = n$ 

$$\blacksquare \text{ for every } i \geq 1, n_i = \begin{cases} n_{i-1}/2 & \text{if } n_{i-1} \text{ even} \\ 3 \cdot n_{i-1} + 1 & \text{if } n_{i-1} \text{ odd} \end{cases}$$

#### Example for n=5

5

## Sequence of natural numbers $n_0, n_1, n_2, n_3, n_4, n_5, \dots$

$$\blacksquare$$
  $n_0 = n$ 

$$\blacksquare \text{ for every } i \geq 1, n_i = \begin{cases} n_{i-1}/2 & \text{if } n_{i-1} \text{ even} \\ 3 \cdot n_{i-1} + 1 & \text{if } n_{i-1} \text{ odd} \end{cases}$$

#### Example for n=5

5, 16

## Sequence of natural numbers $n_0, n_1, n_2, n_3, n_4, n_5, \dots$

$$n_0 = n$$

$$\blacksquare \text{ for every } i \geq 1, n_i = \begin{cases} n_{i-1}/2 & \text{if } n_{i-1} \text{ even} \\ 3 \cdot n_{i-1} + 1 & \text{if } n_{i-1} \text{ odd} \end{cases}$$

#### Example for n=5

5, 16, 8

## Sequence of natural numbers $n_0, n_1, n_2, n_3, n_4, n_5, \dots$

$$\blacksquare$$
  $n_0 = n$ 

#### Example for n=5

5, 16, 8, 4

## Sequence of natural numbers $n_0, n_1, n_2, n_3, n_4, n_5, \dots$

$$\blacksquare$$
  $n_0 = n$ 

#### Example for n=5

5, 16, 8, 4, 2

## Sequence of natural numbers $n_0, n_1, n_2, n_3, n_4, n_5, \dots$

$$\blacksquare$$
  $n_0 = n$ 

#### Example for n=5

5, 16, 8, 4, 2, 1

## Sequence of natural numbers $n_0, n_1, n_2, n_3, n_4, n_5, \dots$

$$n_0 = n$$

#### Example for n=5

5, 16, 8, 4, 2, 1, 4

## Sequence of natural numbers $n_0, n_1, n_2, n_3, n_4, n_5, \dots$

$$\blacksquare$$
  $n_0 = n$ 

$$\blacksquare \text{ for every } i \geq 1, n_i = \begin{cases} n_{i-1}/2 & \text{if } n_{i-1} \text{ even} \\ 3 \cdot n_{i-1} + 1 & \text{if } n_{i-1} \text{ odd} \end{cases}$$

#### Example for n=5

5, 16, 8, 4, 2, 1, 4, 2

## Sequence of natural numbers $n_0, n_1, n_2, n_3, n_4, n_5, \dots$

$$\blacksquare$$
  $n_0 = n$ 

$$\blacksquare \text{ for every } i \geq 1, n_i = \begin{cases} n_{i-1}/2 & \text{if } n_{i-1} \text{ even} \\ 3 \cdot n_{i-1} + 1 & \text{if } n_{i-1} \text{ odd} \end{cases}$$

#### Example for n=5

5, 16, 8, 4, 2, 1, 4, 2, 1

## Sequence of natural numbers $n_0, n_1, n_2, n_3, n_4, n_5, \dots$

$$\blacksquare$$
  $n_0 = n$ 

#### Example for n=5

5, 16, 8, 4, 2, 1, 4, 2, 1, ... (repetition at 1)

## Exercise – The Collatz Sequence

## Write a program that

- $\blacksquare$  takes an integer n as input
- outputs the Collatz sequence using

$$n_0=n$$
 and

$$n_i = \begin{cases} n_{i-1}/2 & \text{if } n_{i-1} \text{ even} \\ 3 \cdot n_{i-1} + 1 & \text{if } n_{i-1} \text{ odd} \end{cases}$$



## Exercise – The Collatz Sequence

```
n = int(input("Compute the Collatz sequence for n = "))
while n > 1:
            # stop when 1 is reached
   if n % 2 == 0: # n is even
      n //= 2
                   # n is odd
   else:
      n = 3 * n + 1
   print(n, end=" ")
```

#### Example for n = 27

27 82 41 124 62 31 94 47 142 71 214 107 322 161 484 242 121 364 182 91 274 137 412 206 103 310 155 466 233 700 350 175 526 263 790 395 1186 593 1780 890 445 1336 668 334 167 502 251 754 377 1132 566 283 850 425 1276 638 319 958 479 1438 719 2158 1079 3238 1619 4858 2429 7288 3644 1822 911 2734 1367 4102 2051 6154 3077 9232 4616 2308 1154 577 1732 866 433 1300 650 325 976 488 244 122 61 184 92 46 23 70 35 106 53 160 80 40 20 10 5 16 8 4 2 1

The Collatz Concecture

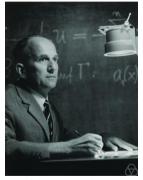
[Lothar Collatz, 1937]

For every  $n \ge 1$ , 1 will occur in the sequence

The Collatz Concecture

[Lothar Collatz, 1937]

For every  $n \ge 1$ , 1 will occur in the sequence



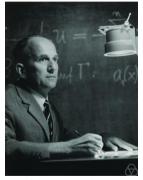
Lothar Collatz [Wikimedia]

The Collatz Concecture

[Lothar Collatz, 1937]

For every  $n \ge 1$ , 1 will occur in the sequence

Nobody could prove the conjecture so far



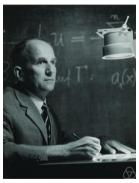
Lothar Collatz [Wikimedia]

The Collatz Concecture

[Lothar Collatz, 1937]

For every  $n \ge 1$ , 1 will occur in the sequence

- Nobody could prove the conjecture so far
- If it is wrong, then the while loop for computing the Collatz sequence can be an endless loop for some n as input



Lothar Collatz [Wikimedia]

# Thanks for your attention

