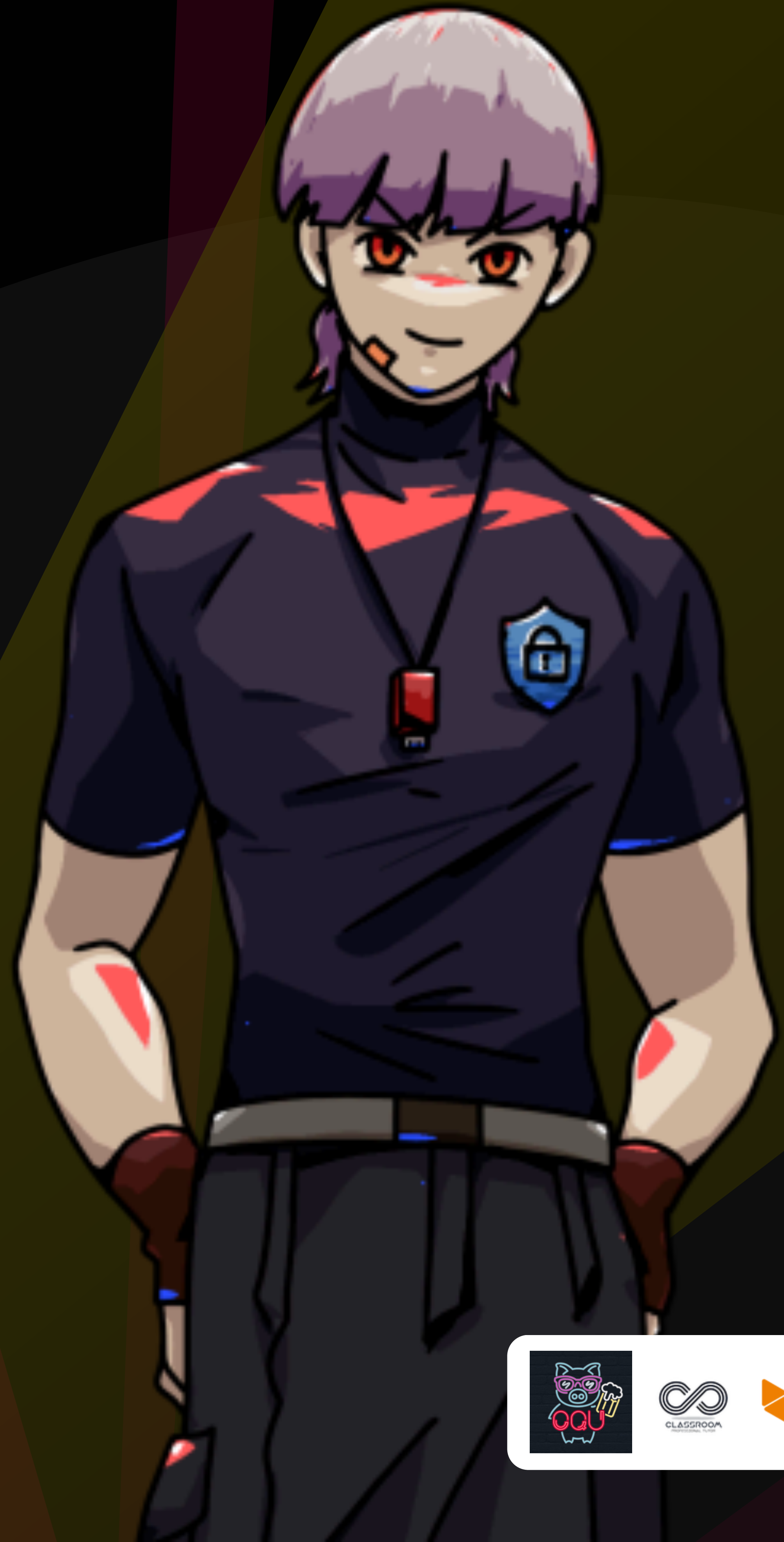
ModCom Freshy mystery 2024

Number Theory

ทฤษฎีจำนวน ชวนปวดหัว

TOPICS

- Divisibility and Modular Arithmetic 01
- Integer Representations and Algorithms 02
- GCD and LCM 03



Divisibility and Modular Arithmetic

Divisibility

หากเรามีจำนวนเต็ม **a** และ **b** ใดๆ (โดยที่ $a \neq 0$) เราจะสามารถระบุได้ว่า **a** หาร **b** ลงตัว (**a** divides **b**) หรือ **b** หารด้วย **a** ลงตัว (**b** is divisible by **a**) เมื่อเราสามารถหาจำนวนเต็ม **c** ใด ๆ ที่ทำให้

b > a

$$b = ac$$

โดยเราจะใช้สัญลักษณ์ **a | b** เพื่อบ่งบอกว่า **a** หาร **b** ลงตัว

Properties of Divisibility

1. หากตัวตั้ง (ตัวถูกหาร) มี **a** เป็นตัวประกอบแล้ว **a** จะหารตัวตั้งดังกล่าวได้ลงตัว

$$a \mid ab$$

$a|ab \Rightarrow \frac{ab}{a} = b$

Properties of Divisibility

2. หาก **a | b** แล้ว **a | bc** เมื่อ **c** เป็นจำนวนเต็มใด ๆ

$a = 2$, $b = 4$, $c = 3$

$a|b$; $2|4 = 2$ จริง

$bc = 4 \times 3 = 12$

$a|bc$; $2|12 = 6$ จริง

Properties of Divisibility

3. หาก **a | b** และ **b | c** แล้ว **a | c**

ถ้า $a = 2$, $b = 4$ และ $c = 8$

$a|b \Rightarrow 2|4 = 2$ "จริง"

$b|c \Rightarrow 4|8 = 2$ "จริง"

$a|c \Rightarrow 2|8 = 4$ "จริง"

Properties of Divisibility

4. หาก **a | b** และ **a | c** แล้ว **a | (b ± c)**

$a = 2, b = 4, c = 8$

$a|b \Rightarrow 2|4 = 2$ "จริง"

$a|c \Rightarrow 2|8 = 4$ "จริง"

$b+c \Rightarrow 4+8 = 12$

$b-c \Rightarrow 4-8 = -4$

$a|b+c \Rightarrow 2|12 = 6$ "จริง"

$a|b-c \Rightarrow 2|-4 = -2$ "จริง"

Properties of Divisibility

ข้อควรระวัง!!!

บทกลับของสมบัติที่กล่าวมาข้างต้น อาจไม่เป็นจริงเสมอไป

$a \mid b+c \rightarrow a \mid b$ และ $a \mid c$

ex $a = 2$, $b = 3$, $c = 1$

$b + c = 3 + 1 = 4$

$a \mid b+c$; $2 \mid 4 = 2$ "จริง"

$a \mid b$; $2 \mid 3 = 1$ เศษ 1 "เท็จ"

Divisibility

Example Problem

จงหาค่าของ **a** ที่เป็นจำนวนเต็มบวก ซึ่งทำให้ **a | a + 4**

Sol^n $a \mid a+4 = \dfrac{a+4}{a}$

$= \dfrac{a}{a} + \dfrac{4}{a} = 1 + \dfrac{4}{a}$

ตัวประกอบ $4 = 1, 2, 4$

$6 = 1, 2, 3, 6$

$\therefore a = 1, 2, 4$

The Division Algorithm

เมื่อ a เป็นจำนวนเต็มใด ๆ และ d เป็นจำนวนเต็มบวก เราจะสามารถกล่าวได้ว่า

"ตัวหาร"

ผลหาร

"ตัวตั้ง"

เศษ

$$a = dq + r$$

โดยที่ q เป็นจำนวนเต็มซึ่งเป็นผลหารของ a ÷ d

r เป็นจำนวนเต็มบวกซึ่งเป็นเศษจากการหารของ a ÷ d และ $0 \le r < d$

The Division Algorithm

จากสมการ **a = dq + r** เรามักใช้สัญลักษณ์ต่อไปนี้แทน “ผลหาร” และ “เศษจากการหาร”

หาค่าผลหารโดยไม่สนเศษ

$$q = b\ \mathbf{div}\ a$$ — (Integer Division)

$$r = b\ \mathbf{mod}\ a$$ — (Modulo Operator)

ค่าเศษโดยไม่สนผลหาร

The Division Algorithm

Example Problem

จงหา**ผลหาร**และ**เศษ**จากการหาร 2567 ด้วย 38

$$
\begin{array}{r}
67 \\
38\,\overline{)\,2567} \\
-\underline{228} \\
287 \\
-\underline{266} \\
21
\end{array}
$$

67 = 2567 div 38 #

21 = 2567 mod 38 #

The Division Algorithm

Example Problem

จงหา**ผลหาร**และ**เศษ**จากการหาร -34 ด้วย 3

Solⁿ

$$
\begin{array}{r}
-11 \\
3\,\overline{)\,-34} \\
-33 \\
\hline
\cancel{-1}
\end{array}
\rightsquigarrow 0 \le r < d
$$

$$
\begin{array}{r}
-12 \\
3\,\overline{)\,-34} \\
-36 \\
\hline
2
\end{array}
$$

$-12 = -34 \text{ div } 3$

$2 = -34 \bmod 3$

The Division Algorithm

Example Problem

จง**พิสูจน์**ว่า ถ้า **a** เป็นจำนวนที่ 3 หารไม่ลงตัว แล้ว 3 หาร **(a+1)(a+2)** ลงตัว

$a = 3q + r$

a แทน $(a+1)(a+2)$; $(3q+r+1)(3q+r+2)$

$a = 3q + r$

r เกิดขึ้น $1, 2$

แทน $r = 1$

$(3q+2)(3q+3) = 3(3q+2)(q+1)$

แทน $r = 2$

$(3q+3)(3q+4) = 3(q+1)(3q+4)$

ดังนั้น $3 \mid (a+1)(a+2)$

The Division Algorithm

Example Problem

จง**พิสูจน์**ว่า ถ้า **a** เป็นจำนวนเต็มบวก แล้ว 4 จะหาร **a² + 2** ไม่ลงตัว

Sol^n กรณี 1 $a =$ คู่

$a = 2k \; ; \; k \in \mathbb{Z}^+ \quad \mathbb{N}$

$a^2 + 2 = (2k)^2 + 2 = 4k^2 + 2$

$4 \mid a^2 + 2 \; ; \; \dfrac{a^2+2}{4} = \dfrac{4k^2+2}{4} = \dfrac{4k^2}{4} + \dfrac{2}{4}$ ไม่ลงตัว

The Division Algorithm

Example Problem

จง**พิสูจน์**ว่า ถ้า **a** เป็นจำนวนเต็มบวก แล้ว 4 จะหาร **a² + 2** ไม่ลงตัว

กรณี 2 a = จำนวนเต็มคี่ = $2k+1$

$$a^2+2 = (2k+1)^2+2$$

$$= 4k^2+4k+3$$

$4 \mid a^2+2 \rightsquigarrow \frac{a^2+2}{4} = \frac{4k^2+4k+3}{4} = \frac{4k^2}{4}+\frac{4k}{4}+\frac{3}{4}$

ไม่ลงตัว

สรุป $4 \mid a^2+2$ ไม่ลงตัว

Congruence Relation

เมื่อเศษจากการหารจำนวนเต็ม **a** และ **b** ด้วย **m** มีค่าเท่ากัน

$$a \bmod m = b \bmod m$$

เราจะกล่าวว่า “**a** เป็น congruence กับ **b** modulo **m**”

$$a \equiv b \pmod{m}$$

Congruence Relation

Example Problem

จงทดสอบว่า 125 congruent กับ 5 mod 6 หรือไม่

$$125 \bmod 6 = 5 \bmod 6$$

$$5 = 5$$

สรุปได้ว่า $125 \equiv 5 \pmod{6}$

Congruence Relation

Properties of Modulo

"บวก"

1. $(a+b) \bmod m \;=\; ((a \bmod m) + (b \bmod m)) \bmod m$

"คูณ"

2. $(ab) \bmod m \;=\; ((a \bmod m)(b \bmod m)) \bmod m$

Congruence Relation

Example Problem

กำหนดให้ $a \equiv 11 \pmod{19}$
และ $b \equiv 3 \pmod{19}$

จงหาค่าของ c ที่ทำให้ $c \equiv 7a + 3b \pmod{19}$ โดยที่ $0 \leq c \leq 18$

Sol^{n} $a \equiv 11 \ (\mathrm{mod}\ 19)$

$7a \equiv \big((7 \bmod 19)(\overset{11}{\cancel{a}} \bmod 19)\big) \bmod 19$

$7a \equiv 77 \bmod 19$

$7a \equiv 1 \bmod 19$

Congruence Relation

Example Problem

กำหนดให้ $a \equiv 11 \pmod{19}$
และ $b \equiv 3 \pmod{19}$

จงหาค่าของ c ที่ทำให้ $c \equiv 7a + 3b \pmod{19}$ โดยที่ $0 \leq c \leq 18$

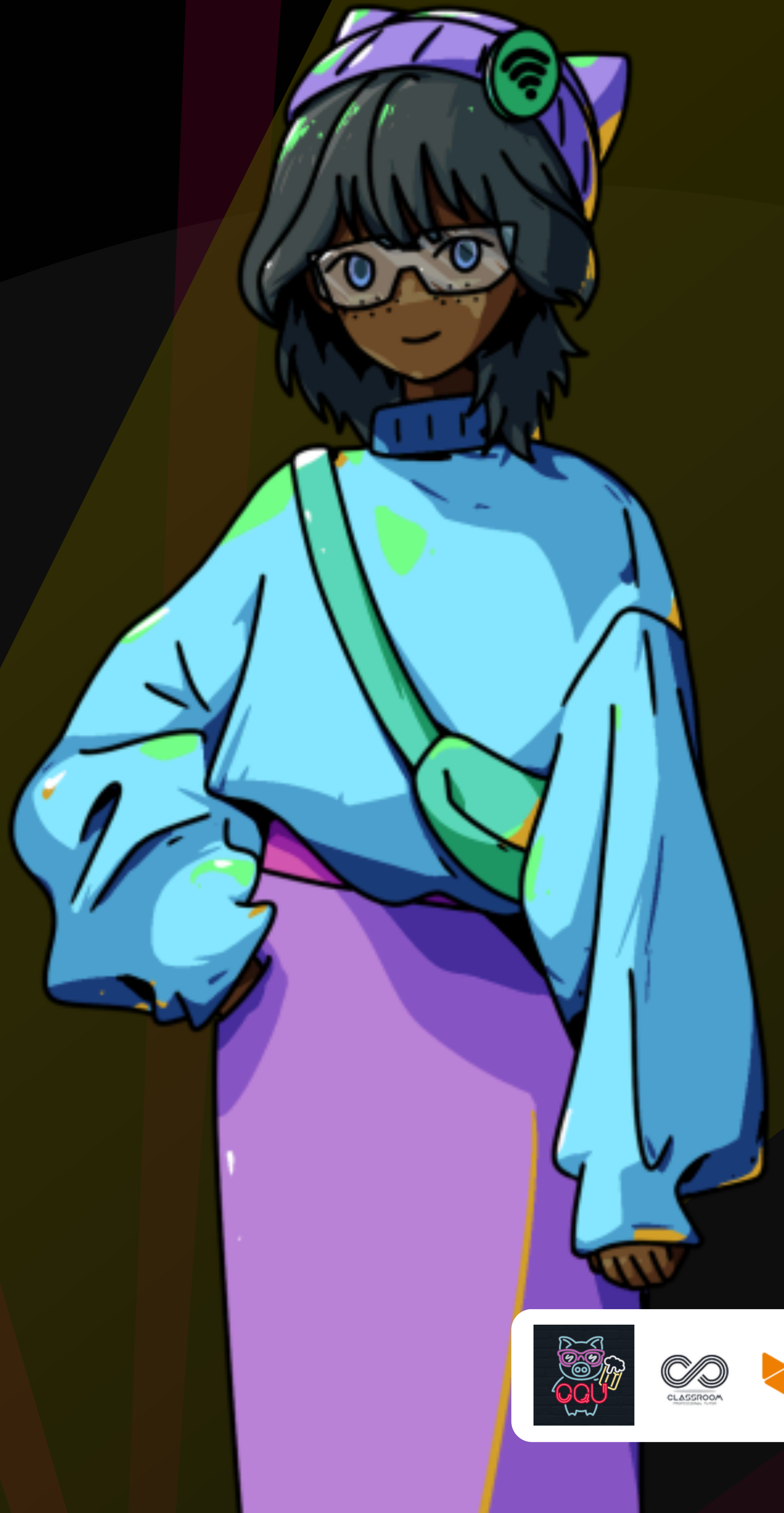
$b \equiv 3 \bmod 19$

$3b \equiv ((3 \bmod 19)(3 \bmod 19)) \bmod 19$

$3b \equiv 9 \bmod 19$

$c \equiv 7a + 3b \pmod{19} \rightsquigarrow$ $c \equiv (1 + 9) \bmod 19$

$c \equiv 10 \bmod 19 \equiv 10$



Integer Representations and Algorithms

Representation of Integers

เราสามารถแสดงตัวเลขต่าง ๆ ได้ด้วยระบบเลขฐานต่าง ๆ ตัวอย่างเลขฐานที่เราใช้กันเป็นประจำ ได้แก่ “เลขฐานสิบ”

$$6945 = 6 \times 10^3 + 9 \times 10^2 + 4 \times 10^1 + 5 \times 10^0$$

Representation of Integers

ในการแสดงเลขฐานต่าง ๆ เราจะแสดงชุดตัวเลขในฐานนั้น ๆ เรียงกันอยู่ในวงเล็บและห้อยเลขฐานกำกับไว้ด้านหลัง (ยกเว้นเลขฐาน 10 ที่มักจะละวงเล็บและไม่กำกับเลขห้อยเอาไว้)

$$\begin{aligned} n &= (a_k a_{k-1} \cdots a_2 a_1 a_0)_b \\ &= a_k b^k \ + \ a_{k-1} b^{k-1} \ + \ \cdots \ + \ a_2 b^2 \ + \ a_1 b \ + \ a_0 \end{aligned}$$

Base Conversion

Example Problem (base *b* to base 10)

จงแปลงจำนวนต่อไปนี้ให้อยู่ในรูปเลขฐาน 10

$(635)_5 = 6 \times 5^2 + 3 \times 5^1 + 5 \times 5^0$

$= 150 + 15 + 5$

$= 170$

$(DE2)_{16} = 13 \times 16^2 + 14 \times 16^1 + 2 \times 16^0$

$= \square$

11 ; A = 10

12 ; A, B = 10, 11

16 ; A, B, C, D, E, F = 10, 11, 12, ..., 15

Base Conversion

Example Problem (base 10 to base *b*)

จงแปลง 425 ให้อยู่ในรูปเลขฐาน 8

$$
\begin{array}{r|l}
8 & 425 \\ \hline
8 & 53 \quad R\ 1 \\ \hline
 & 6 \quad R\ 5
\end{array}
$$

651_8

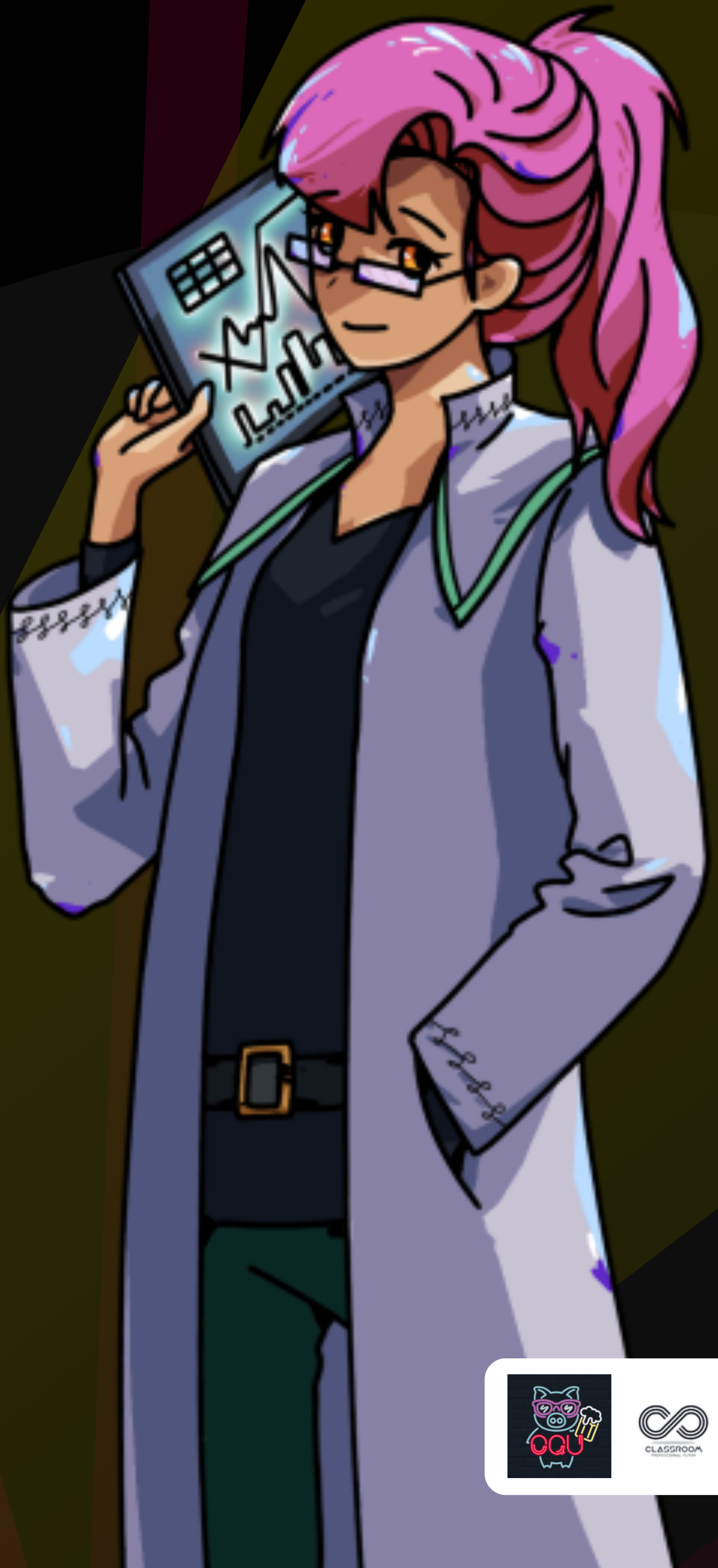
Base Conversion

Example Problem (base 2 to base 2^n)

จงแปลง $(11111010101100)_2$ ให้อยู่ในรูปเลขฐาน 8

$$
\begin{array}{ccccc}
 & & & & 4\ 2\ 1 \\
11 & 111 & 010 & 101 & 100 \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
3 & 7 & 2 & 1\times 2^2 + 1\times 2^0 = 5 & 1\times 2^2 = 4
\end{array}
$$

$\text{Ans} = 37254_8$



GGD and LGM

Great Common Divisor

ตัวหารร่วมมาก (GCD) คือการหาจำนวนเต็มที่มากที่สุด ที่หารทั้ง a และ b ได้ลงตัว โดยเราสามารถเขียนสัญลักษณ์แทนการหา **gcd** ของ a และ b ได้ **gcd(a, b)**

Great Common Divisor

Example Problem (GCD)

$$\gcd(\underbrace{2^3 3^5 5^7}_{a}, \underbrace{2^5 11^2}_{b}) = ?$$

$a = 2^3 \times 3^5 \times 5^7$

$b = 2^5 \times 11^2$

$2^5 = 2^2 \cdot 2^3$

หรมของ a,b = 2^3 #

Least Common Multiplier

ตัวคูณร่วมน้อย (LCM) คือการหาจำนวนเต็มที่มากที่สุด ที่ทั้ง a และ b สามารถหารจำนวนดังกล่าวได้ โดยเราสามารถเขียนสัญลักษณ์แทนการหา **lcm** ของ a และ b ได้

lcm(a, b)

Least Common Multiplier

Example Problem (LCM)

$$lcm(\underbrace{2^3 3^5 5^7}_{a}, \underbrace{2^5 11^2}_{b}) = ?$$

$a = 2^3 \times 3^5 \times 5^7$

$b = 2^5 \times 11^2$

ครน $= 2^5 \times 3^5 \times 5^7 \times 11^2$

ครน $(a,b) = 2^5 \times 3^5 \times 5^7 \times 11^2$

Relation of GCD and LCM

$$ab = \gcd(a,b) \times \text{lcm}(a,b)$$

Example

ถ้า a = 12 และ b = 18 จงหาค่าของ gcd(a,b) และ lcm(a,b) และตรวจสอบว่า

$$ab = \gcd(a,b) \times \text{lcm}(a,b)$$

$\gcd(12,18) = 6$

$\text{lcm}(12,18) = 36$

$12 \times 18 = 6 \times 36$

$216 = 216$

Euclidean Algorithm

Euclidean Algorithm เป็นการหา **gcd** รูปแบบหนึ่ง ที่นิยมอย่างมากในการใช้หาคำตอบ ในกรณีที่เราจะต้องเขียนโปรแกรมคอมพิวเตอร์ โดยหลักการสำคัญของการทำ **Euclidean Algorithm** จะมี คือ

สมมติให้เราต้องการหา **gcd(a, b)** โดยที่ a มีค่ามากกว่า b เราจะนำ b มาหาร a ซึ่งจะเขียนได้อยู่ในรูปของ **a = bq + r** โดยที่ q เป็นผลหาร และ r เป็นเศษจากการหาร

1. ในกรณีที่ r ไม่เป็น **0** (หรือเป็นการหารที่ไม่ลงตัว) เราจะได้ว่า **gcd(a, b) = gcd(b, r)**
2. ในกรณีที่ r เป็น **0** (หรือเป็นการหารที่ลงตัว) เราจะได้ว่า g**cd(a, b) = b**

Euclidean Algorithm

Example Problem (Euclidean Algorithm)

จงหา gcd(1071, 462) โดยใช้ Euclidean Algorithm

1.

$$1071 = 462(2) + 147$$

$$462 = 147(3) + 21$$

$$147 = 21(7) + 0$$

หรม $(1071, 462) = 21$

2.

2	1071	462	3
	924	441	
7	147	21	
	147		
	0		

หรม $(1071, 462) = 21$