Modular Arithmetic

↳ special kind of numbers
  ↳ nos in a modular space.

Remainders — is 117 divisible by 4?

$$\frac{117}{4} = 29\frac{1}{4}$$

$$117 = 29 * 4 + 1$$

$$\frac{\text{dividend}}{\text{divisor}} = \text{quotient} \quad \frac{\text{remainder}}{\text{divisor}}$$

remainder ≥ 0

$$= \text{dividend} = \text{divisor} * \text{quotient} + \text{remainder}$$

integer integer integer integer

$$117 = 29 * 4 + (1)$$

$$= 30 * 4 + (-3)$$

$117 = 30 \quad \frac{-3}{4}$ ✗

$$\text{remainder} = \%$$

$117 \% 4 = 1$

Modular arithmetic → Cryptography
                  ↳ Hashing

RSA
DES
AES
:

$(N \% m)$ → remainder → integer
↳ divisor ↳ ≥ 0
↳ $<$ divisor

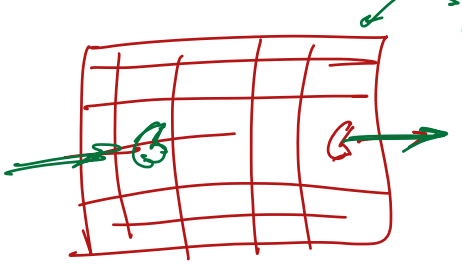
$\frac{117}{4} = 29 * 4 + 1$ ← it cannot be further divided by the divisor

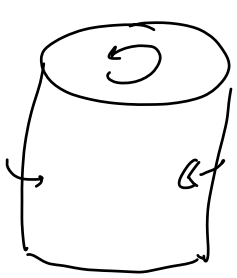
$= 28 * 4 + 5$ ✓

$(N \% m) \in \{0 \dots (m-1)\}$

↳ modulus space of m
set of possible remainders when dividing by m.

$(\% m)$ space → $\{0 \dots (m-1)\}$ $(m-2)(m-1)\,0, 1, 2, \dots (m-1), 0, 1, 2$





$0(\% m) = \{\}$

$(m) \% m \rightarrow 0$

⇒ Dividend = divisor * quotient + remainder

remainder = dividend − (divisor * quotient)

$0 \leq \text{--} < \text{divisor}$

$150\%7 = 150 - (7 * 21)$

$150 - 147$

$= 3$

$150\%7 = 3$ | $150 = 21*7+3$

$150\%11 = 150 - (11 * 13)$

$150 - 143$

$= 7$

$150\%11 = 7$

$100\%7 = 100 - (7 * 14)$

$= 100 - 98$

$= 2$

$100\%7 = 2$

$(-40\%7)$

remainder = dividend − (divisor * quotient)

$(-40\%7) = -40 - (7*(-5))$

$= -40 - (-35)$

$-35 \nleq -40$

$-40\%7 = -5+7 = 2$

$= -40 - (7*(-6))$

$= -40 - (-42)$

$= 2$

$\frac{-40}{7} = -6\frac{2}{7}$ / $-5\frac{-5}{7}$

$-60\%9 = -60 - (9*(-7))$

$= -60 - (-63)$

$= 3$

$-60\%9 = 3$

$-60\%9 = (6) + 9 = 3$

$-40\%7 = -40 - (7 * (-6))$

$= -40 - (-42)$

$= 2$

} tedious.

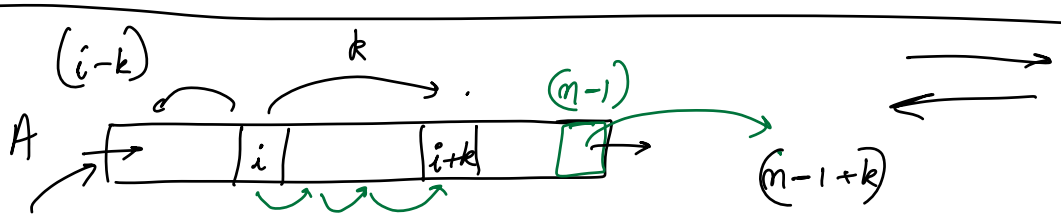
$-40\%7 = -5 + 7 = 2$

$-110\%3 = (-2) + 3 = (1)$

$-110 = -110 - (3 * (-37))$

$= -110 - (-111)$

$= 1$



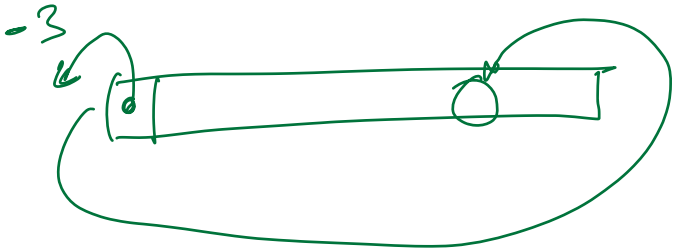
Rotate the array k times to the right

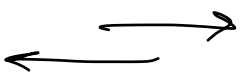
```
for i in range(len(A)):
    if i+k ≥ n:
        B[i+k-n] = A[i]
    else
        B[i+k] = A[i]
```

$B[(i+k)\%n] = A[i]$

$B[(i-k)\%n] = A[i]$

$-ve$





A: | 10 | 20 | 30 | 40 | 50 | 60 |
0 1 2 3 4 5

R clockwise 3 times

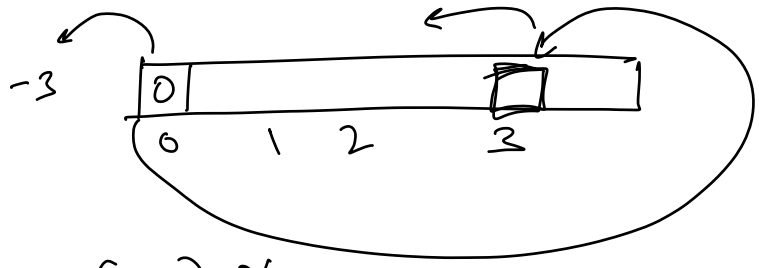
B: | 40 | 50 | 60 | 10 | 20 | 30 |
0 1 2 3 4 5

10 → 0 → 3
20 → 1 → 4
30 → 2 → 5

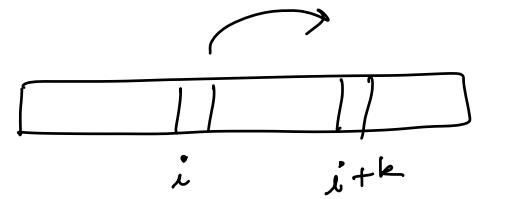
6 → i → (i+3)

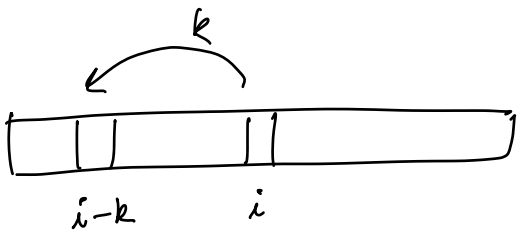
40 → 1 → 6 → 0 — 6 % 6
50 → 4 → 7 → 1 — 7 % 6 ←
60 → 5 → 8 → 2 — 8 % 6

$i \rightarrow i+k$ $\qquad$ $i \rightarrow (i-k)$

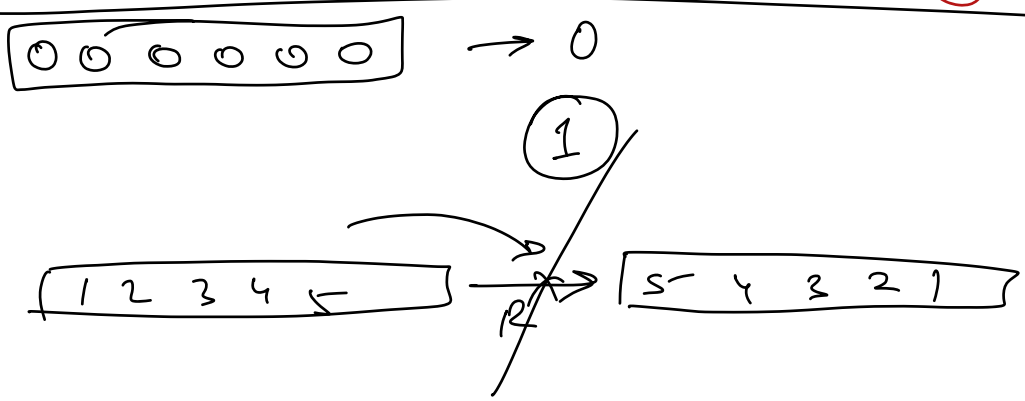


$(0-3)\ \%\ 6 \quad = -3\ \%\ 6 = 3$





$(i-k)\ \%\ m$



Properties of the % operator.

$(50+5) * 10 \quad = \quad 500+50 = 550$

$= 55 * 10 = 550$

Linearity of Remainders

$$(a+b)\ \%\ m = [(a\ \%\ m) + (b\ \%\ m)]\ \%\ m$$

$$(a-b)\ \%\ m = [(a\ \%\ m) - (b\ \%\ m)]\ \%\ m$$

$$(12+17)\ \%\ 10 = (29\ \%\ 10) = 9$$

$$(12\ \%\ 10) + (17\ \%\ 10) = 2 + 7 = (9)\ \%\ 10$$

$$= 9$$

assume that $a = k_1 * m + r_1$

$$b = k_2 * m + r_2$$

$$(a+b) = (k_1 * m + r_1) + (k_2 * m + r_2)$$

$$= (k_1 + k_2) * m + (r_1 + r_2)$$

$$(a+b)\ \%\ m = (r_1 + r_2)$$

$$(a * b)\ \%\ m = [(a\ \%\ m) * (b\ \%\ m)]\ \%\ m$$

$$(40 * 27)\ \%\ 4 = (40\ \%\ 4) * (27\ \%\ 4)$$

$$= 0 * 1$$

$$= 0$$

37
×40
1480 %4

$(43 * 38) \% 4 = (1634) \% 4 = 2$

$[(43\%4) * (38\%4)]\%4$

43
38
1214
42
1634

$= (3 * 2) \% 4$

$= 6 \% 4 = 2$

$(a/b) \% m \neq [(a\%m) / (b\%m)] \% m$

% does Not distribute over division !

a & b are int

a+b → int

a*b

a-b

a/b is int

$\left(\frac{1}{7}\right) \% 3$?

inverse modulous

↳ Adv. DSA.

$$a^n \% m = \left[(a \% m)^n \right] \% m$$

$$a^n = \underbrace{a * a * a * a \cdots a}_{n \text{ times}}$$

$$(a^n \% m) = \underbrace{(a * a * a * \cdots a)}_{n \text{ times}} \% m$$

$$= \underbrace{\left((a \% m) * (a \% m) * (a \% m) \cdots * (a \% m) \right)}_{n \text{ times}} \% m$$

$$= (a \% m)^n \% m$$

$$(43^{37}) \% 4 = 3$$

$$43^{37} \% 4 = \left[(43 \% 4)^{37} \right] \% 4$$

$$= (3^{37}) \% 4$$

$37 = 36 + 1$

$3^{37} = 3^{36+1}$

$$= (9^{18} \cdot 3) \% 4 \qquad = 3^{36} \cdot 3^{1}$$

$$= [(9^{18} \% 4) * (3 \% 4)] \% 4 \qquad = 9^{18} \cdot 3^{1}$$

$$= 9^{19} \cdot 3$$

$$[[(9 \% 4)^{18} \% 4] * 3] \% 4$$

$$((1^{18} \% 4) * 3) \% 4$$

$$= ((1 \% 4) * 3) \% 4 = (1 * 3) \% 4 = 3$$

$$(43^{37} \% 4) = [(44 - 1)^{37}] \% 4$$

$$= [(44 - 1) \% 4]^{37} \% 4$$

$$= (44 \% 4 - 1 \% 4)^{37} \% 4$$

$$= (-1)^{37} \% 4$$

$$= (-1) \% 4$$

$$= 3$$

% 6 space

$-18 \equiv -12 \equiv -6 \equiv 0 \equiv 6 \equiv 12 \equiv 18 \equiv 24 \ldots$

$-17 \equiv -11 \equiv -5 \equiv 1 \equiv 7 \equiv 13 \equiv 19 \equiv 25 \ldots$

if $a \,\%\, m = b \,\%\, m$ $\quad a \neq b$

a behaves like b

$a \equiv b \pmod{m}$

in a calculation $(\%\, m)$ if we have an 'a', we can replace it with a 'b'

$43^{37} \,\%\, 4 \Rightarrow (-1)^{37} \,\%\, 4 = (-1) \,\%\, 4 = 3$

$43 \equiv -1$ $\quad \%\, 4$ space?

$43 \,\%\, 4 = 3$

$-1 \,\%\, 4 = 3$

if $a \equiv b \pmod m$

in a calculation in the $(\%\ m)$ space whenever you have a you can replace it with b

$\%$ C space

$\ldots -12 \equiv -6 \equiv 0 \equiv 6 \equiv 12 \equiv 18 \ldots$

$-11 \equiv -5 \equiv 1 \equiv 7 \equiv 13 \equiv 19$

$-4 \equiv 2 \equiv 8 \equiv 14$ —

$-3 \equiv 3 \equiv 9 \equiv 15$ —

$-2 \equiv 4 \equiv 10 \equiv 16$ —

$-1 \equiv 5 \equiv 11 \equiv 17$

$$(43^{37}) \% 21 \equiv (1^{37}) \% 21 = 1$$

$21 * 2 = 42$

$$(43^{37}) \% 38 = (5^{37}) \% 38$$

$43 = 5 \% 38$ $= (25^{18} \cdot 5) \% 38$

$$= (25\%38)^{18} \cdot (5\%38)$$

$$= (625)^9 \cdot 5\%38$$

$$= 17^9 \cdot 5$$

$$= 289^4 \cdot 17 \cdot 5$$

$\frac{625}{38} = 17$

TC - O(P)

SC - O(1)

$(n^p \% m)$

$O(\log_2 P)$

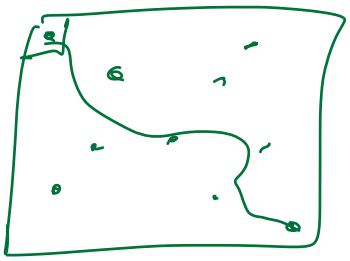
```
def pow(n, p, m):
    # return (n^p % m)
    n = n % m
    ans = 1
    for i in range(p):
        ans = (ans * n) % m

    return ans
```

---

given —

return ans % (10^9+7)



proof of computation
& not the actual result.

43^{37}

int / double / long.

50 digits

$(43^{37})\%\ m$

% → proof of computation
↳ avoid overflow.

---

if $a < b$ and a is not -ve
then $a \% b = ?$ a

$3 \% 7 = 3$

10:37 → 10:50

10:45 →

$$(a+b)\%m = [(a\%m) + (b\%m)]\%m$$

$(17+18)\%10$

$35\%10$

$=5$

$= [(17\%10) + (18\%10)]\%10$

$= (7+8)\%10$

$= (15)\%10$

$= 5$

---

given a string → integer

$S =$ " 1 3 2 6 8 7 1 1 0 7 6 3 5 4 "

$m \rightarrow$ int

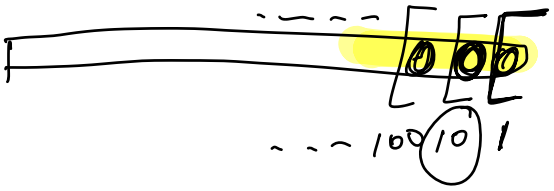
$s\%m$

$S = 4*10^0 + 5\times10^1 + 3\times10^2 + 6\times10^2 + \cdots$

$S\%m$

$(S\%m) = (4\times10^0)\%m + (5\times10^1)\%m + (3\times10^2)\%m + \cdots$

$(4\%m) * (10^0)\%m + (5\%m) * (10^1)\%m + \cdots$




```
def mod(s, m):
    ans = 0
    coefficient = 1

    for i in reversed(range(len(s))):
        d = int(s[i])
        ans = (ans + ((d % m) * coeff) % m) % m
        coeff = (coeff * 10) % m

    return ans.
```

---

100 10 1

s = 1 3 2 6 8 7 1 1 0 7 6 3 5 4 $\quad \%_0 7$

```
def mod(s, m):
    ans = 0
    coefficient = 1

    for i in reversed(range(len(s))):
        d = int(s[i])
        ans = (ans + ((d % m) * coeff) % m) % m
        coeff = (coeff * 10) % m

    return ans.
```

ans = ~~0~~ 4 + 1 + 6

coeff = ~~X X X~~ 6

coef = 1

for every digit

coef = (10 * coef)

do something with (coeff % m)

m = 7

coef = 1 → (1%7) = 1

= 10 %7 → (10%7) = 3

= 100 %7 → (100 %7) = 2

= 1000 %7

= 10000 %7

|

100%7 ≠ (10%7)

= ((10%7) * (10%7))%7

---

ans = 0

pow = 0

for each digit from the right

coeff = 10**pow

ans = ans + (digit * coeff)% m

pow += 1

10000 ← 0000

100 10 1

≡

ans = 0

coeff = 1

for each digit from the right

ans = ans + (digit * coeff) % m

coeff = (10 * coeff) % m

$c = 10 \% 7 = 3$

$(10 \% 7) \% 7 = 3$

$((10 \% 7) \% 7) \% 7 = 3$

---

divisibility rules

decimal = base 10 $\Rightarrow$ $10 = 2 \times 5$

divisibility by 2 $\rightarrow$ last digit is a multiple of 2

$[abcdef] = a*10^5 + b*10^4 + \dots + e*10^1 + f$

divisible by 2, 5

divisibility test for 5 $\rightarrow$ last digit must be divisible by 5

7126387297060 $\vdots$ 5

divisibility test for 4. $= 2^2 \rightarrow$ last 2 digits

$abcdef = \underbrace{(abcd) \cdot 100}_{x} + \underbrace{e*10+f}$

$= 5^2 = 25 \rightarrow$ last 2 digits

8, 125 → last 3 digits

16, 625 → last 4 digits

---

125 divisible by 8? ✗

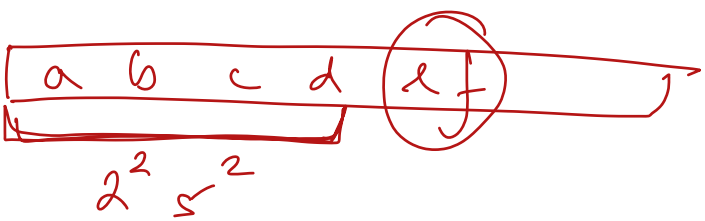
100 " " 8? ✗

2000 " " " ? ✓

1000 " " " ? ✓

10000 " " 4? ✓

$2 \cdot 5$ (1, 2) ? $= 50$



2 → 1

5 → 1

10 → 1

4 → 2

25 → 2

50 → 2

100 → 2

20 → 2

8 → 3

125 → 3

250 → 3

500 → 3

40 → 3

200 → 3

10 = 2 * 5

base - ~~12~~ 60

divisibility by

2, 3, 5

Divisibility by 3 → sum of digits must be divisible by 3

$abcdef = a \cdot 10^5 + b \cdot 10^4 + c \cdot 10^3 + d \cdot 10^2 + e \cdot 10^1 + f$

$\%3 \quad = (a \cdot 10^5)\%3$

$= (a\%3) \cdot (10^5\%3)$

$(10\%3)^5$

$10\%3 = 100\%3 = 1000\%3 \overset{!}{=} 2 \text{ -- } 1$

$= (a+b+c+d+e+f)\%3 \quad = 1$

$10 \% 9 = 1$

$100 \% 9 = 1$

check if sum of digits is a multiple of 9.

---

divisibility test for 11

diff b/w the sums of even & odd digits must be a multiple of 11

1357663

$1+5+7+6+3 = 22$

$3+7+5+6+1 = 22$

$22 - 22 = 0$

$10^1 \% 11 = -1$

$(10^2 \% 11) = 1$

$(abcdef) \% 11$

$(10 \% 11) \equiv -1$

$(10^2 \% 11) \equiv (+1)$

$= a \cdot 10^5 + b \cdot 10^4 + c \cdot 10^3 + d \cdot 10^2 + e \cdot 10^1 + f$

$= a \cdot (-1) + b(+1) + c(-1) + d(+1) + e(-1) + f(+1)$

---

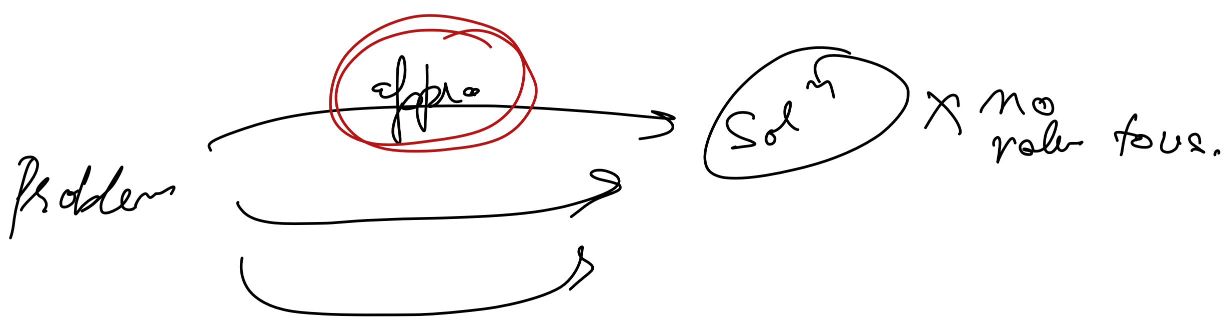
divisibility test in base 7

$10 \% 11 = 10$

$10 \% 11 = 10$

$-1 \% 11 = 10$

$(10 \equiv -1) \% 11$



given a no. check if it is a magic no or not.

if you add the digits of the no → n2

" " " " " n2 → n3

⋮

Single digit no.

1 → magic

○ → not magic

```
def is_magic(n):
    while n > 9:
        s = 0
        n2 = n
        while n2 > 0:
            s += n2 % 10
            n2 //= 10
        n = s
    return n == 1
```

wrong bcoz

```
def is_magic(n):
    return n % 9 == 1
```

(11)

1
2
4
8
16

(1)

---

(1) question has poor language?
↳ report to us
fixed.

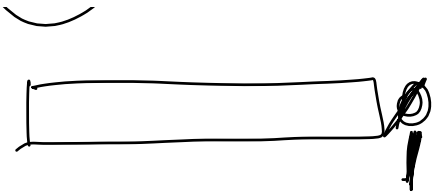
(2) it is difficult for me to understand the question
- (1) improve comprehension
- (2) looking at examples

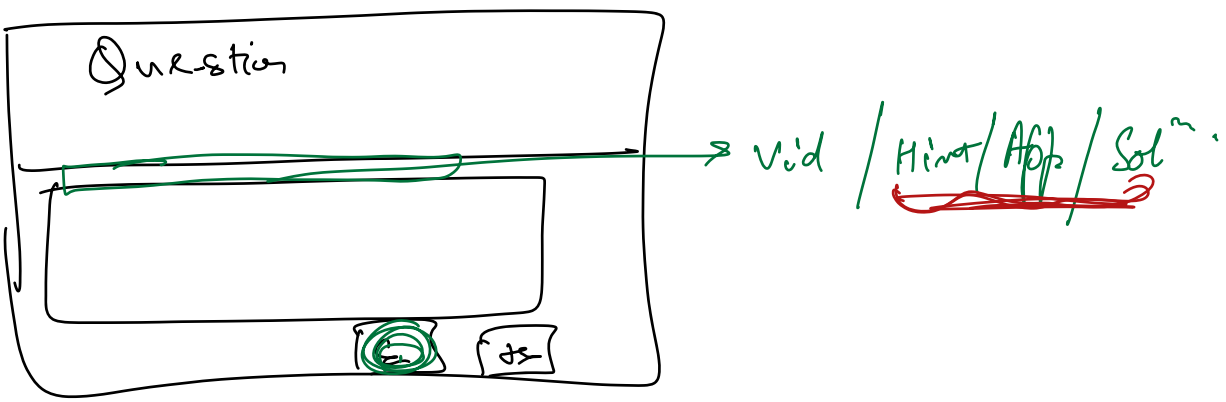
A
(11) = (1011)

0 → 1 → 2 → 4 → 5 → 10 → 11
1 0 0 1 0 1

1 0 1 1

(*2) +1 (*2) (+1)





(1) some question in class → approach (logic)
↳ assign ↓ code

(2) logic yourself → neo

approaching a problem

(1) Read question carefully
(2) Read & understand given examples
(3) Sample test cases yourself

(4) Brute force

(5) Observations.

(6) Optimize → ok for now!

↑

adv. DSA

12768 226

divisible by 8?

12768 000 1000/8 = 125

236 is divisible by 8?

---

tables upto 12x12

Squares upto 20^2

Cubes upto 11^3

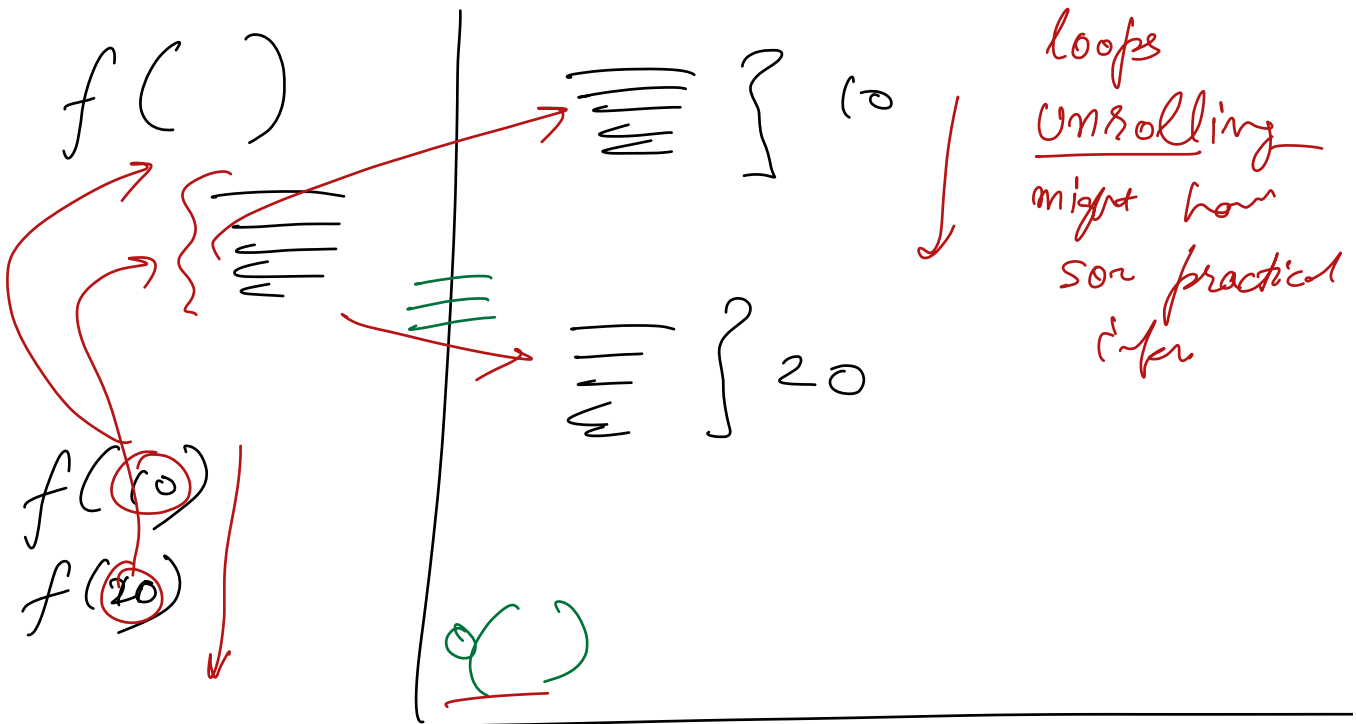
divisibility rules of 2, 3, 4, 5, 6, 8, 9, 10, 11

Spaced Repetition Software (SRS)

Anki

→ never forget something.

DRY → Don't Repeat Yourself



---

① Implementation ← via practice

Brute force is not clear.

② optimial is not obvious.

---

remainder = dividend − (divisor * quotient)

≥ 0

$\frac{40}{-5}$ $\quad$ $\frac{41}{-5}$

$40 \% (-5) = 40 - ((-5) * -8)$

$= 40 - 40 = 0$

$41 \% (-5) = 41 - ((-5) * (-8))$

$= 41 - 40$

$= 1$

$(-40 \% 3) = 2$

$2 \rightarrow (-1) + 3 = 2$

Pragya → noun

Pragya → girls name

Pragya → boys name.

↳ adjective