Primitive root and Discrete root

Special class

Nishchay Manwani • Dec 28, 2020

Primitive root and Discrete root

Nishchay Manwani

zevs-orz

EnEm

28-12-2020

Let's crack Competitive Programming together!

Prerequisites

- modular operations
  - $(5+3) \% 6 \Rightarrow 2$
  - mod 6
- modular exponentiation $\rightarrow (2^5) \% 7 \rightarrow 4$
- modular inverse $\rightarrow (2 \times 4) \% 7 \rightarrow 1$
  - $4 = 2^{-1} \% 7$

↳ Euler's totient func

≃ Fermat's little theorem

CODECHEF | unacademy

EXCLUSIVE BATCH ANNOUNCED

EnEm

Intermediate Batch : GOING LIVE THIS DECEMBER

Refer & Earn Invite Friends And Win 10% Discount On Subscription

If Referred Person Subscribes For A Month
You Get A Week Of Extension On Your Current Subscription

- Structured Learning Path To Get Placed In FAANG Companies
- Industry Accepted Codechef Certification On Course Completion
- Elite Educator Panel Consisting Of ICPC Finalists, Codeforces Grandmasters And Alumni Of Top Product Companies Like Google, Facebook And Linkedin

Basics
↓
inter
↓
adv

Exclusive INTERMEDIATE Batch Starting on 22nd Dec

Structured learning for intermediates to become expert level coders

Instructors: Highly competent technical minds with **ICPC world finals, IOI medals**, IOI team training experience and **Codeforces Grandmasters** as accolades

Develop end to end subject matter expertise required to get placed in top product firms or create your own tech company or crack international coding contests

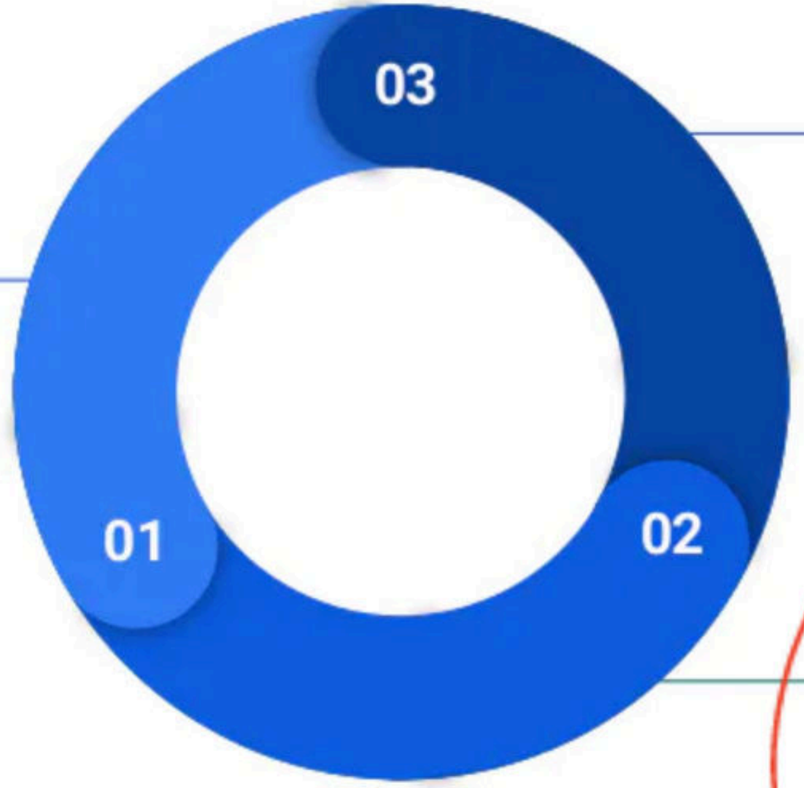
Industry accepted **Codechef Certification** upon successful course completion

The expense is even lesser than INR 90/ day with our 1 year subscription to avail all of it

What you will get

Live Interactive Classes

Attend live interactive classes with our top educators.



Doubt Support

Get your doubts resolved by our expert panel of teaching assistants and community members

Practice Relevant Problems @ CodeChef

Each class comes with a set of curated practice problems to help you apply the concepts in real time.

Topic-wise Batch Structure

C++ Java python

Week	Topic
Week 1-4	Sorting and Searching- Concepts and Problem Solving
Week 5-10	Data Structures- Concepts and Interview Problem Solving
Week 11-15	Additional Concept in C++
Week 16-17	Greedy Algorithms with Classical Problem Solving
Week 18-20	Data Structures 2 - Square Root Decomposition and Advanced Problems
Week 21-22	Number Theory and Interview Questions
Week 23-25	Recursion and DP Concepts and Handpicked Problem Solving
Week 26-30	Discrete Mathematics in C++- Concept to Problems
Week 30-34	Graph Algorithms- Advanced Problems
Week 35-37	Segment Trees
Week 38-40	Advanced Dynamic Programming
Week 41-43	Computational Geometry
Week 44-52	ICPC Regionals + World Finals Problem solving

Educators

Tanuj Khattar

ACM ICPC World Finalist - 2017, 2018. Indian IOI Team Trainer 2016-2018. Worked @ Google, Facebook, HFT. Quantum Computing Enthusiast.

Sanket Singh

Software Development Engineer @ LinkedIn | Former SDE @ Interviewbit | Google Summer of Code 2019 @ Harvard University | Former Intern @ISRO

Pulkit Chhabra

Codeforces: 2246 | Codechef: 2416 | Former SDE Intern @CodeNation | Former Intern @HackerRank

Riya Bansal

Software Engineer at Flipkart | Former SDE and Instructor @ InterviewBit | Google Women TechMakers Scholar 2018

Triveni Mahatha

Qualified ICPC 2016 World Final. Won multiple Codechef Long Challenges (India). ICPC Onsite Regionals' Problem setter and Judge. IIT Kanpur.

Deepak Gour

ICPC World Finalist 2020 | Former Instructor @InterviewBit | Software Engineer at AppDynamics

Educators

Himanshu Singh

World Finalist ICPC 2020, Winner Techgig Code Gladiators 2020, Winner TCC '19, 2020 CSE Graduate from IIT BHU, Works at Nutanix

Nishchay Manwani

Hey I am Nishchay Manwani from CSE, IIT Guwahati and I'm a Seven star on Codechef and International Grandmaster on Codeforces.

Murugappan S

Software engineer at Google. Have won many programming contests. Max Rating of 2192 in codeforces and 2201 in codechef.

Vivek Chauhan

Codechef: 7 stars (2612) India Rank 6, Codeforces: MASTER (2279), Won Codechef Long Challenges(India), TCO20 Southern Asia Runner up

and many more joining soon...

Teaching Assistants support on chat and Doubts Forum

CODECHEF Discuss

You may face issue with markdown in posts. In such cases, report it here along with the post link.

unacademy Live Classes / CodeChef Practice & Doubts / CodeChef Doubt Forum

Clear your Doubts with our Expert Panel of Teaching Assistants & Community Members

Leave no room for doubts. Create a topic.

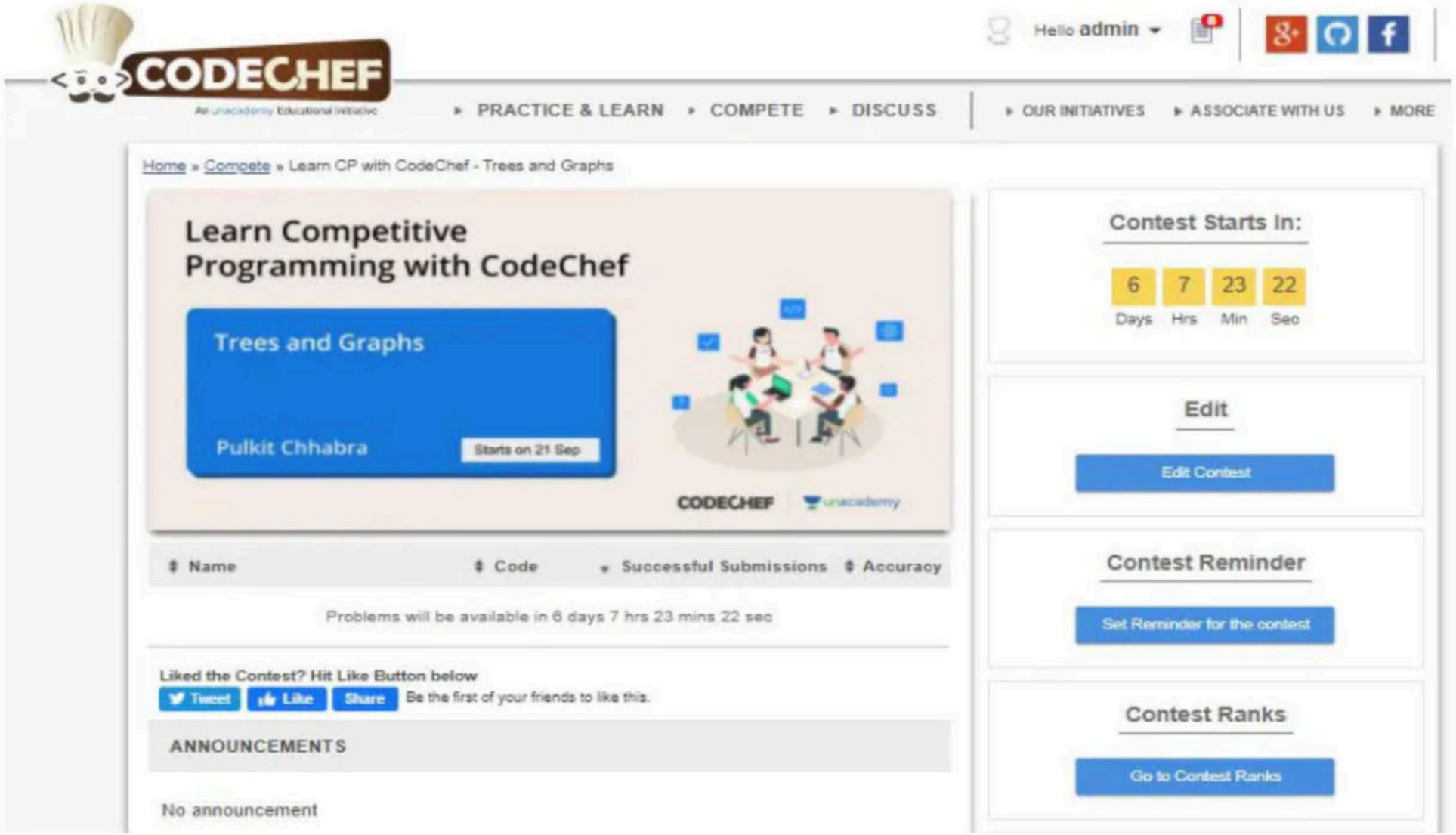
CODECHEF unacademy

Learn CP on Unacademy Plus | all tags | Latest | Top | Bookmarks | Edit | + New Topic

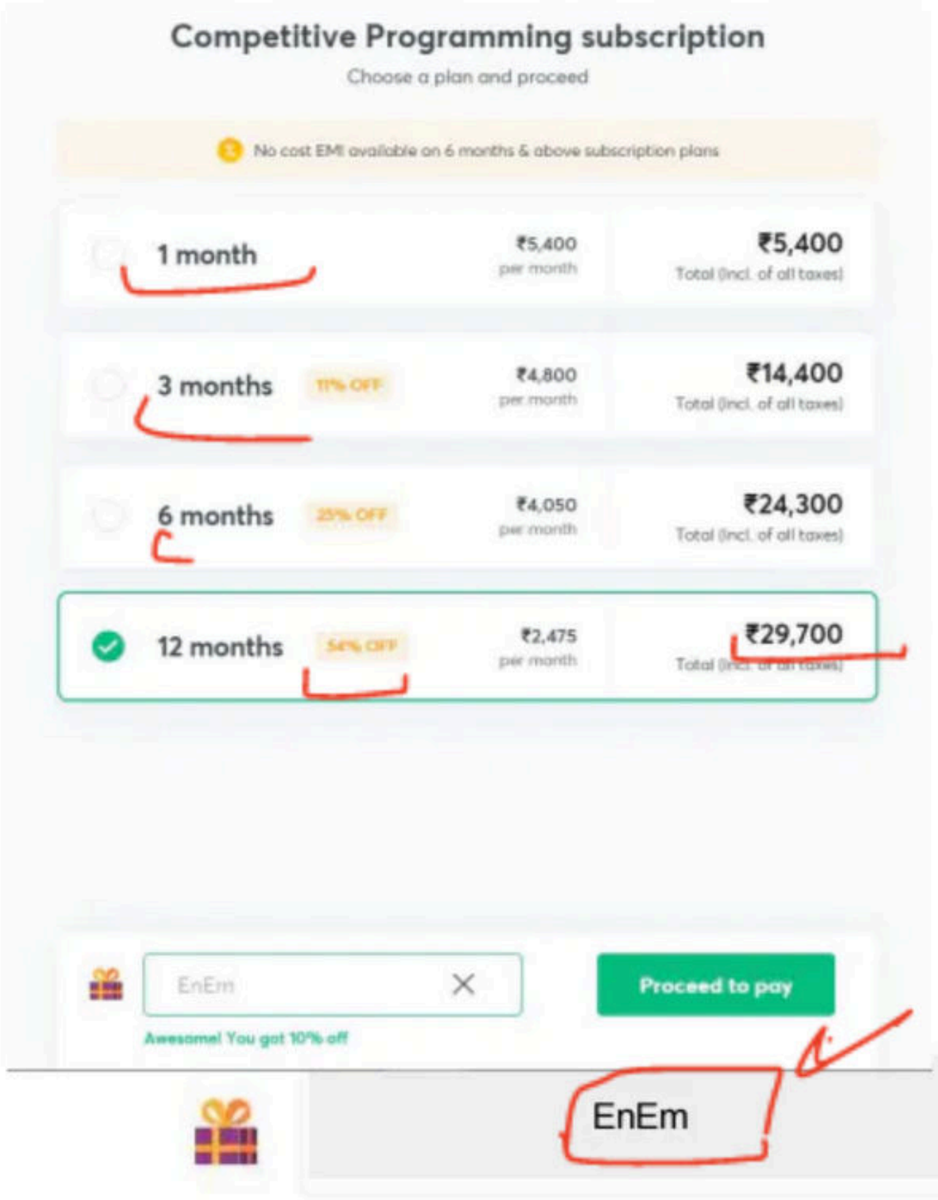
Topic	Replies	Views	Activity
About the Learn CP on Unacademy Plus category	1	6	2d

There are no more Learn CP on Unacademy Plus topics. Why not create a topic?

Course-wise Practice Problems



Flexible Subscription Plans



Euler's totient function

phi

↳ $n \longrightarrow \phi(n)$

of x such that $\gcd(x, n) = 1$

$1 \le x \le n$

$\phi(4) \to 2$

1 ✗ 3 ✗

$\phi(5) \to 4$

1 2 3 4 ✗

$$\hookrightarrow \boxed{\left(a^{\phi(b)}\right) \% b \equiv 1}$$

Fermat's little theorem

↳ $\gcd(a, b) = 1$

How many such numbers exist where if the number is 0<=x<12 & (x^4) mod 12 = 1

A. 1

B. 2

C. 3

D. 4

$x^n \bmod 12 = 1$

x	0	1	2	3	4	5	6	7	8	9	10	11
x^n	0	1	16	-	-	-	-	-	-	-	-	-
$x^4 \%12$	0	1	4	9	4	1						

$3^4 \%12$ $9^2 \%12$ $81 \%12$ $81-12$

$4^4 \%12$ $16^2 \%12$ $4^2 \%12$ 1

A B C D

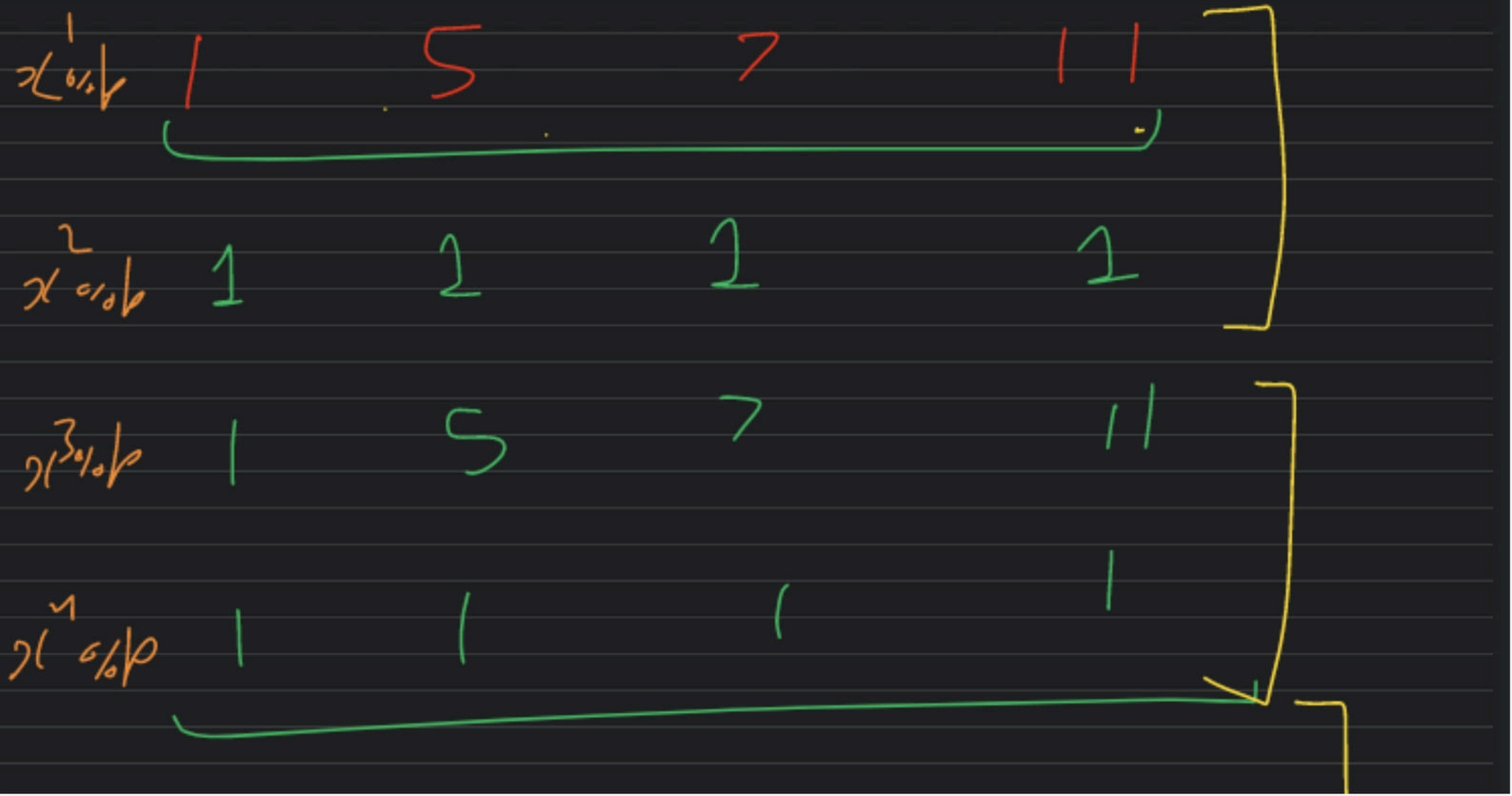
$$\phi(12) = 4$$

1 2 3 4 5 6 7 8 9 10 11

2 2 3 3

$$\text{If } n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

$$\text{then } \phi(n) = n \times \left(1 - \frac{1}{p_1}\right) \times \left(1 - \frac{1}{p_2}\right) \times \cdots \left(1 - \frac{1}{p_k}\right)$$


1 5 7 11
1 1 1 1
1 5 7 11
1 1 1 1

$$x^{n} \quad x^{3} \quad x^{2} \quad x$$

$$1 \quad \infty$$

$$\phi(9) \rightarrow 9 \times \left(1 - \frac{1}{3}\right) \Rightarrow 6$$

$$9 \rightarrow 3^2$$

$$x^{\phi(9)} \% 9 = 1$$

$$\gcd(x, 9) = 1 \rightarrow \phi(9)$$

How many such numbers exist where if the number is 0<=x<9 & (x^6) mod 9 = 1

A. 4

B. 5

C. 6

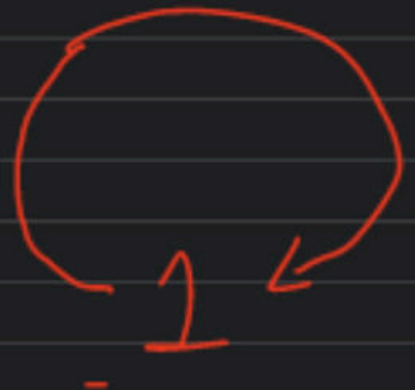
D. 7

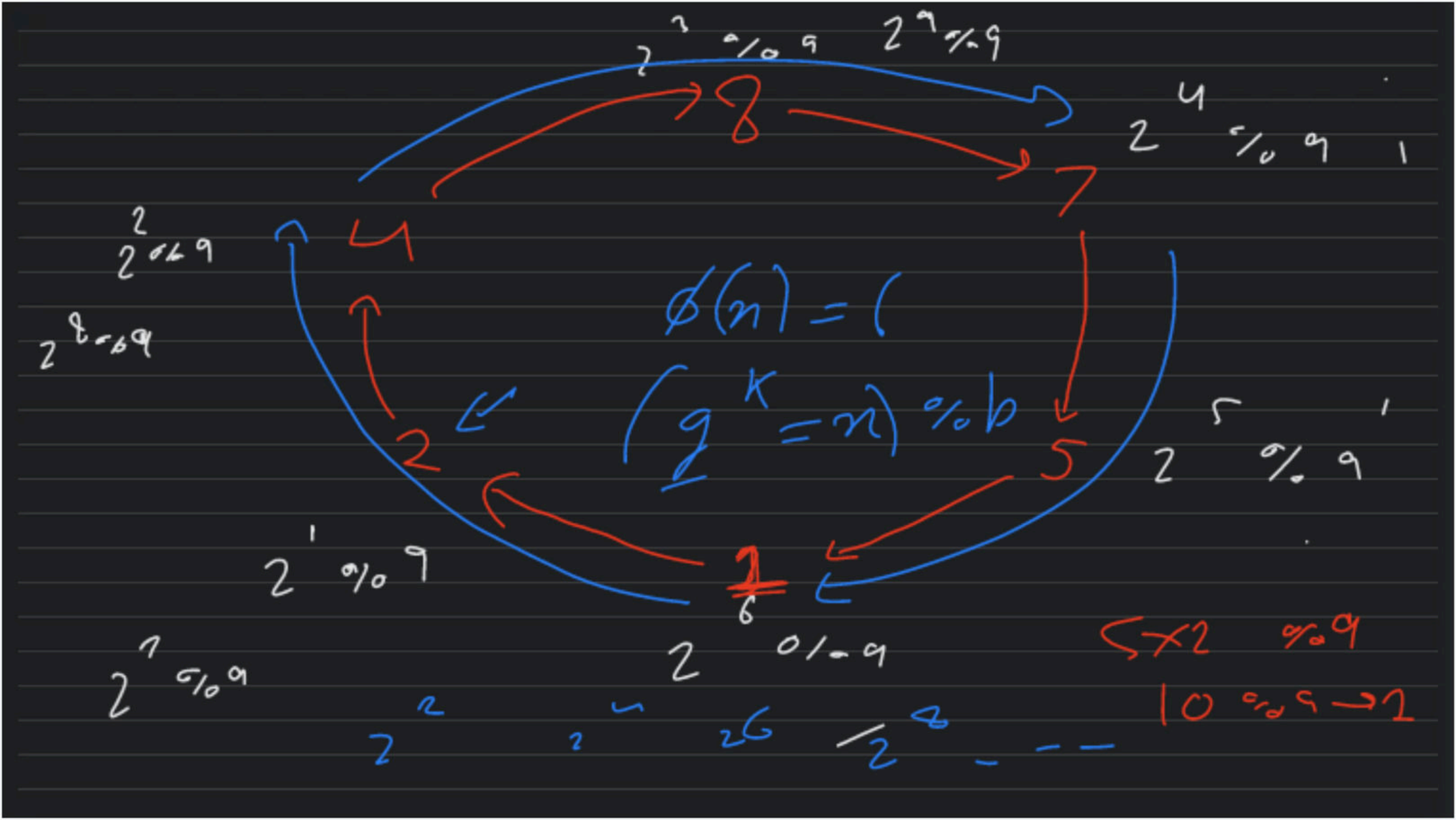
0 1 2 3 4 5 6 7 8

A B C D

$1 \times 1 \% 9$

$1^k \% 9$




$\phi(n) = ($
$(g^k = n) \% b$
$2^3 \% 9$
$2^9 \% 9$
$2^4 \% 9$
$2^2 \% 9$
$2^8 \% 9$
$2^5 \% 9$
$2^1 \% 9$
$2^7 \% 9$
$2^0 \% 9$
$5 \times 2 \% 9$
$10 \% 9 \to 1$

2^5 2^{10} 2^{15} — — —

5 5^2 5^3 — — —

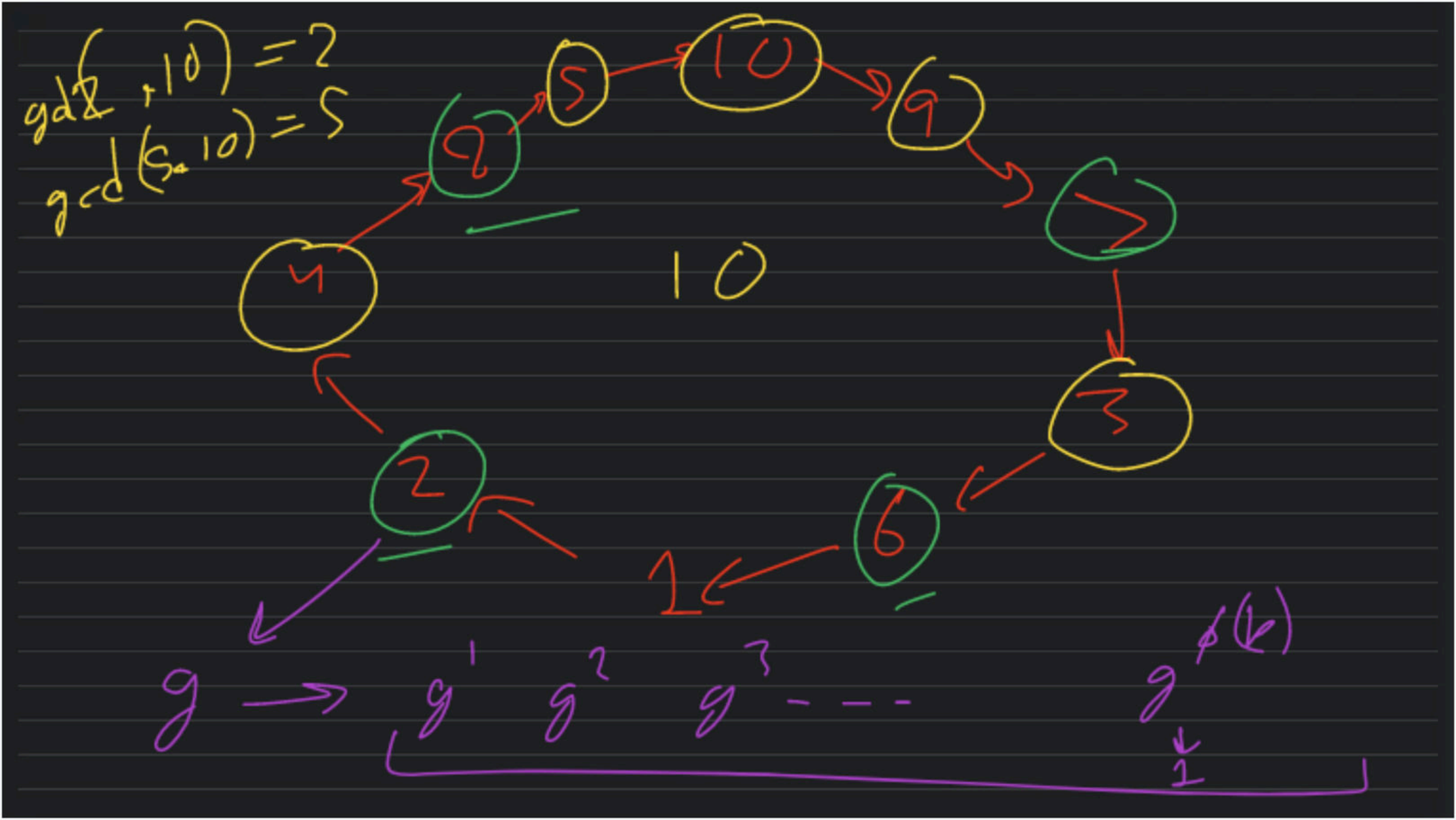
x is 11

$x \quad x^2 \quad x^3 \quad \_ \quad \_ \quad \_ \quad x$

$2 \rightarrow 4 \rightarrow 8 \rightarrow 5 \rightarrow 10$

7 ↓

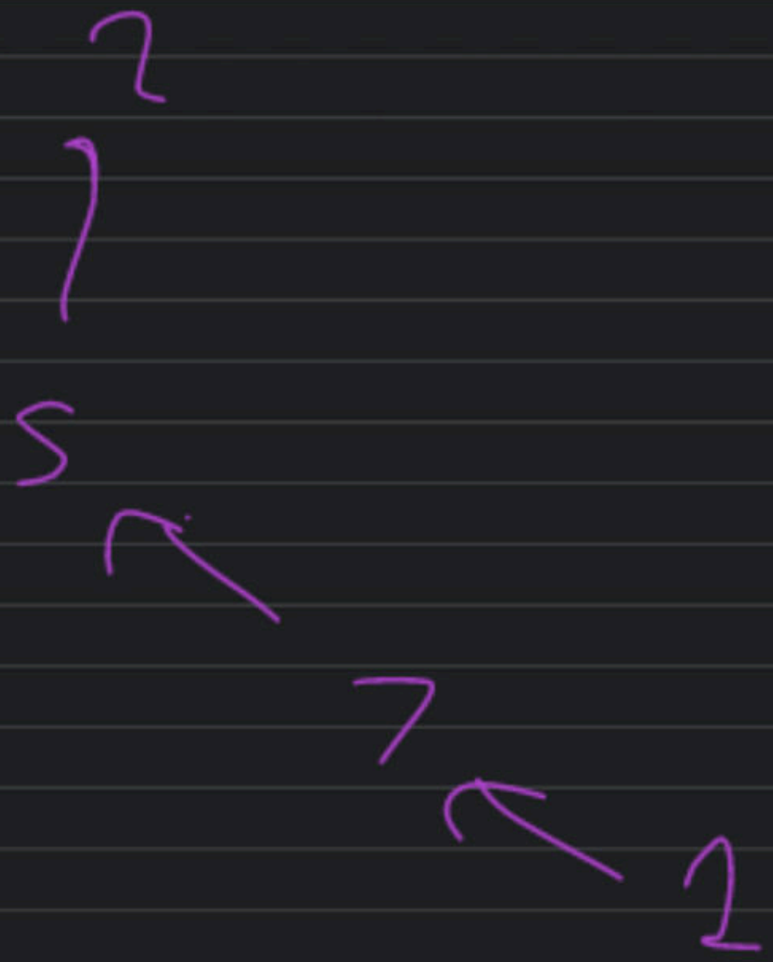
$1 \leftarrow 6 \leftarrow 3 \leftarrow 7 \leftarrow 9$


gcd(7,10) = 2
gcd(5,10) = 5
10
1
g
g^1 g^2 g^3 - - -
$g^{\phi(k)}$
1

$g^{*} = g^{k}$ where $g \perp d(k, \phi(p))$

$= 1$

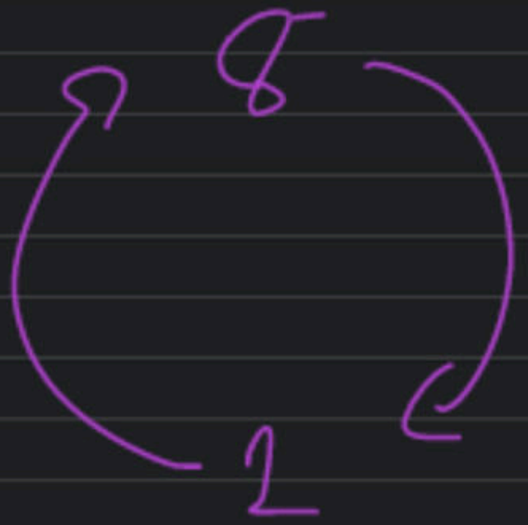
↳ $\perp \phi(\phi(p))$



2 7 5 7 8 7

7^3 2^6 7^9 2^{12}

5 9 8^2 8^7 4^4



A number g where

$g^1 \bmod p, g^2 \bmod p, g^3 \bmod p \ldots$

$\ldots$ generates all such x such that $\gcd(x, p) = 1$

primitive use

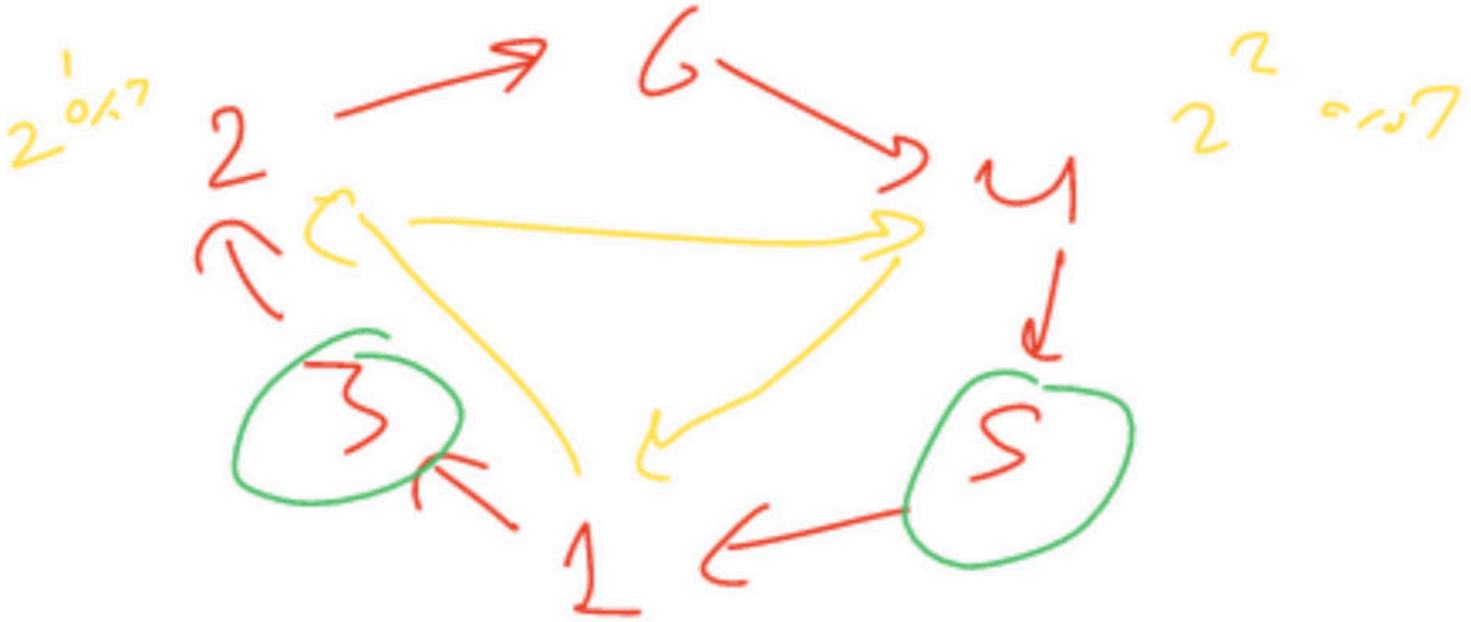
How many such generators are there for p=7?

A. 0

B. 1

C. ~~2~~

D. 3



$\phi(7) \rightarrow 6$

$\phi(6) \rightarrow 6 \times \left(1-\frac{1}{2}\right) \times \left(1-\frac{1}{3}\right) \Rightarrow 6 \times \frac{1}{2} \times \frac{2}{3}$

$\Rightarrow 2$

$$\phi\left(\phi\left(p\right)\right)$$

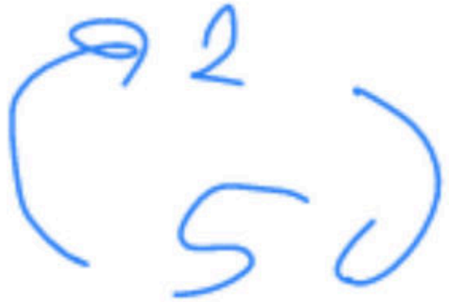
How many such generators are there for p=6?

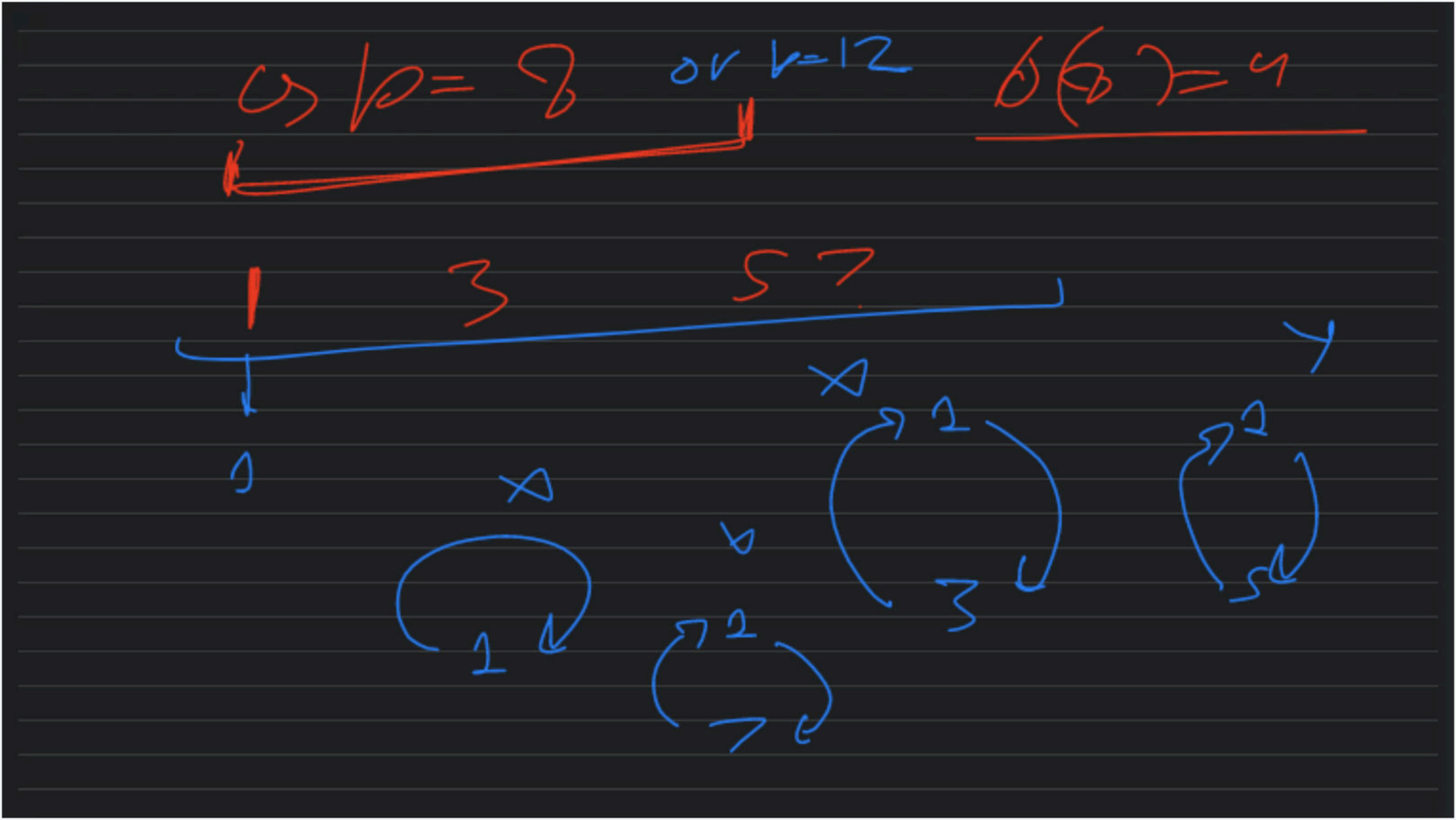
A. 0

B. 1

C. 2

D. 3




p = 2 or 12
δ(6) = 4
1 3 5 7
1
x
1
3
y
2
x
1
b
2
7
2
5

Existence of prim roots

↳ $p = 1$ or $p = 2$ or $p = 4$

↳ or $p = (\text{prime})^k$

↳ or $p = 2 \times (\text{prime})^k$

> 2

$\phi(\phi(p))$

> 2

odd prime

$\mathbb{G}$ $p = 1$ or 2 or 4

$\mathbb{G}$ $p = (\text{odd prime})^k$

$\mathbb{G}$ $p = 2 \times (\text{odd prime})^k$

$\mathbb{G}$ $\phi(\phi(\phi))$ else

FFT → NTT

fast fourier transform

~~Arithmetic~~ number theoritic transform

discrete root

What is x in (x^2) mod 7 = 2?

$0 \leq x < 7$

A. 3 → $9 \not\equiv 7$

B. 6

C. 4 → $4^2 \bmod 7 \rightarrow 2 \rightarrow 16 \neq 2$

D. 5

baby step giant step

prime

$a \left(x^{k} = n \right) \bmod p$

$\hookrightarrow (g^{y})^{k} = n \bmod p$

$\hookrightarrow (g^{k})^{y} = n \bmod p$

$\hookrightarrow t^{y} = n \bmod p$ $O(\sqrt{p})$

$p \rightarrow$ prime

$gcd(a, p) = 1$

$\hookrightarrow [1, p-1]$

$1 \quad \text{---} \quad g$

$g, g^2, g^3, \ldots, g^{\phi(p)}$

$O(p \times g)$

$\hookrightarrow$ $g^d \bmod p \neq 1$ $\forall$ $d \mid \frac{p-1}{\phi(p)}$

$g^d \Rightarrow 1$ $\rightarrow$ not prim root

$g^d \neq 1 \; \forall \; d \mid p-1$ $\rightarrow$ prim root

$d \neq p-1$

$O(r(p-1)) + O(\text{no. of divisors of } p-1 \times \log p \times 8)$

$p-1 \Rightarrow p_1^{a_1} \times p_2^{a_2} \cdots p_k^{a_k}$

$\Rightarrow g^{\frac{p-1}{p_1}} \neq 1$ prim root ✓

$g^{\frac{p-1}{p_2}} \neq 1$

$\vdots$

$g^{\frac{p-1}{p_k}} \neq 1$

$O(\sqrt{p} + g \times (\log p)^2)$

discrete root + trees

discrete log