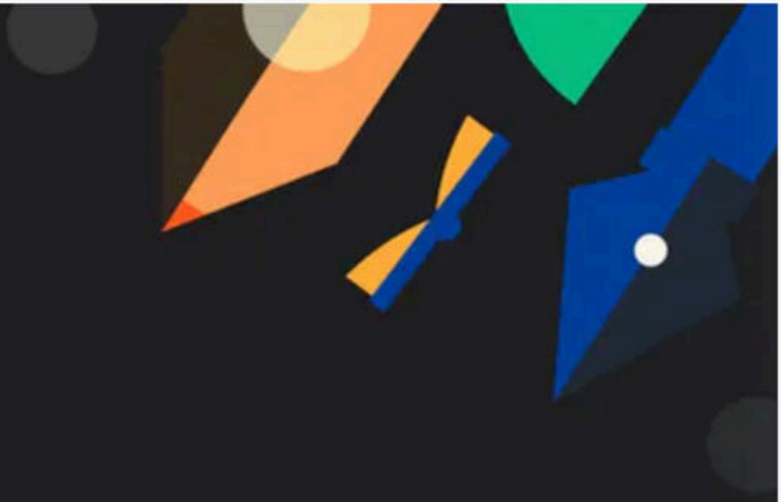


Basics of Modular Arithmetic in C++

Special class

Nishchay Manwani • Oct 5, 2020

Modular Arithmetic

Number Theory

Course on Unacademy

Let's crack Competitive Programming together!

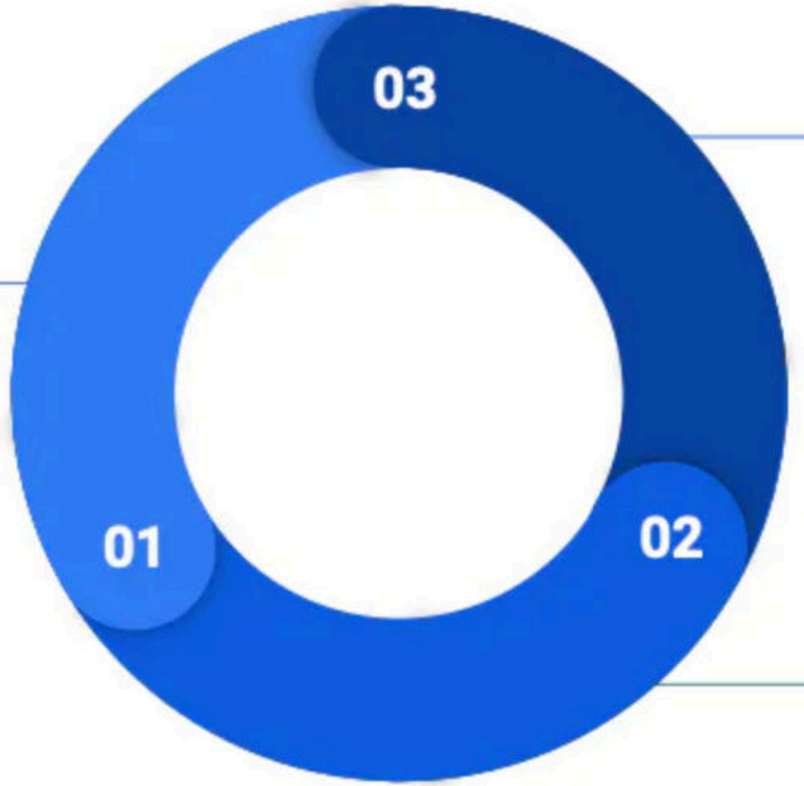
Nishchay Manwani

- zeus_orz at codeforces.com
- EnEm at codechef.com
- Educator at Unacademy : https://unacademy.com/@EnEm

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.

Educators

- **Curated faculty** with a strong **background in competitive programing** & hands on experience of educational training.
- Highly competent technical minds with **ICPC world finals, IOI medals,** IOI team training experience and Codeforces Grandmasters as accolades.
- Alumni of the most respected technology teams from around the world. (Google, Flipkart, Linkedin, Facebook, Amazon, Goldman Sachs, AppDynamics)
- Young & dynamic faculty to make each class as engaging as they are informative.

Educators

Deepak Gour

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

Himanshu Singh

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

Arjun P

I am an IOI 2015 bronze medallist, and my team qualified for the upcoming ICPC 2020 World Finals to be held in Moscow, Russia.

Murugappan S

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

Triveni Mahatha

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

Tanuj Khattar

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

Educators

Riya Bansal

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

Sanket Singh

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

Nishchay Manwani

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

Pulkit Chhabra

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

and many more joining soon...

Topic-wise structure

Beginner	• Introduction to programming • C++ Foundation	• Java Foundation • Python Foundation
Intermediate	• Basic Data Structures • STLs • Sorting and Searching • Greedy Algorithms	• Basic Data Structures 2 • Number Theory • Recursion and DP
Advanced	• Segment Trees • Trees and Graphs • Advanced Dynamic Programming	• Graphs 2 • Computational Geometry
Misc	• ICPC Regionals + World Finals problem solving	

Upcoming Courses

ENGLISH INTERMEDIATE

Course on Greedy Algorithms

Starts on Sep 21, 2020 • 8 lessons

Murugappan S

HINDI ADVANCED

Detailed Course on Graphs - I

Starts on Sep 21, 2020 • 9 lessons

Pulkit Chhabra

HINDI INTERMEDIATE

Course on Introduction to Number Theory

Starts on Sep 22, 2020 • 8 lessons

Nishchay Manwani

Upcoming Courses

ENGLISH BEGINNER

Course on Recursion and Dynamic Programming

Starts on Sep 22, 2020 • 12 lessons

Arjun P

ENGLISH INTERMEDIATE

Course on Sorting and Searching

Starts on Sep 22, 2020 • 10 lessons

Riya Bansal

HINDI INTERMEDIATE

Course on Standard Template Library (STL) in C++

Starts on Sep 23, 2020 • 11 lessons

Sanket Singh

Upcoming Courses

HINDI INTERMEDIATE

Course on Basic Data Structures - I

Starts on Sep 26, 2020 • 11 lessons

Deepak Gour

HINDI INTERMEDIATE

Course on Data Structures (Square Root Decomposition)

Starts on Sep 26, 2020 • 5 lessons

Tanuj Khattar

HINDI BEGINNER

Course on Introduction to Competitive Programming with C++

Starts on Sep 26, 2020 • 10 lessons

Triveni Mahatha

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.

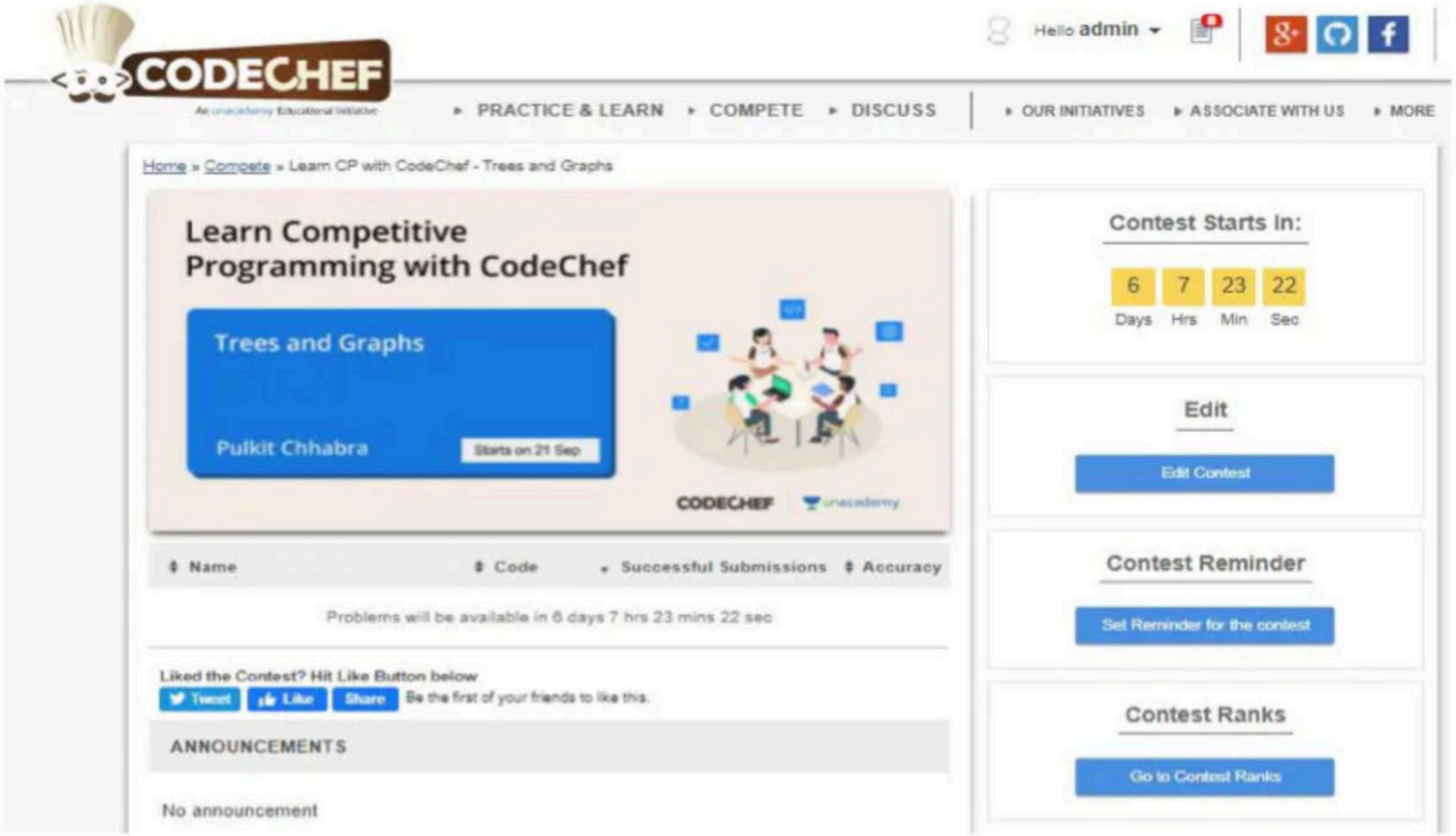
CODECHEF | unacademy

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

1 month	₹999 per month	₹999 Total (Incl. of all taxes)
6 months	₹4,050 per month	₹24,300 Total (Incl. of all taxes)
12 months	₹2,475 per month	₹29,700 Total (Incl. of all taxes)

EnEm

Proceed to pay

Upcoming Free Classes Schedule on website

FREE

Live Classes

Experience Plus for free and start learning from the best

See all

Disjoint Set Union - II

Today, 7:00 PM

Pulkit Chhabra

Discussion on Merge Sort &...

Today, 9:00 PM

Riya Bansal

Headstart to Strings in STL

Today, 10:00 PM

Sanket Singh

ICPC past problems

Sep 19, 2020, 3:30 PM

Himanshu Singh

Modular arithmetic

$a \% b$

$a \bmod b$

$$b \overline{)\, a \;\; q} \qquad a - qb = r$$

- addition
- substraction
- division
- product
- exponentiation

$$0 \leq r < b$$

$$a = b \times q + r$$

$$0 \leq r < b$$

$$q = \left\lfloor \frac{a}{b} \right\rfloor \qquad q \in \mathbb{Z}$$

$$r = a - b \times \left\lfloor \frac{a}{b} \right\rfloor$$

$a \,\%\, b$

$a \bmod b$

$\Big\}$ $\longrightarrow$ r

$$a \,\%\, b = a - b \times \left\lfloor \frac{a}{b} \right\rfloor$$

Ex. $7 \% 4 = 7 - 4 = 3$

$4 \times 1 = 4$

Ex. $2 \% 3 = 2 - 0 = 2$

$3 \times 0 = 0$

Ex. $36 \% 16 = 36 - 32 = 4$

$16 \times 2 = 32$

Addition

1. if $a \% m = b \% m$

then $(a+c) \% m = (b+c) \% m$

$\forall c \in \mathbb{Z}$

Ex. $10 \% 3 = 1$ $\quad b \to 7$

$7 \% 3 = 1$ $\quad m \to 3$

$a \to 10$

$15 \% 3 = 12 \% 3 = \underline{0}$

2. If $a \% m = b \% m$ and $c \% m = d \% m$

↳ $a - \left\lfloor \frac{a}{m} \right\rfloor \times m + a \cdot \left\lfloor \frac{a}{m} \right\rfloor \times m$

↳ $(a + c) \% m = (b + d) \% m$

3. ↳ $(a + b) \% m = ((a \% m) + (b \% m)) \% m$

$a - \left\lfloor \frac{a}{m} \right\rfloor \times m + b - \left\lfloor \frac{b}{m} \right\rfloor \times m$

$(a - b - \left(\left\lfloor \frac{a}{m} \right\rfloor + \left\lfloor \frac{b}{m} \right\rfloor \right) \times m) \% m$

$a = 1.5 \times 10^9$ int

$b = 1.6 \times 10^9$ < int

c++

a%m
0 ≤ _ < m

$a + b \Rightarrow 3.1 \times 10^9$

int ≤ 2×10^9

10^9

% m

$(1.5 \times 10^9 + 1.6 \times 10^9) \% m$

↳ $(1.5 \times 10^9 \% m)$ $(1.6 \% m)$

< m < m

$n \rightarrow 10^5$

$a_i \rightarrow 10^9$

$1 \le i \le n$

int ans = 0

$a_1 + a_2 - - - - a_n$ > int

ans = 0

ans += a_1

ans %= m

ans += a_2

ans %= m

m = $10^9 + 7$ most famous prime in CP.

[998244353]

ans < m

ans < m + 10^9

ans < m

Subtraction

Ans $(-3\%5)$

$\Rightarrow -3$

C++ ans

$5\sqrt{3}$

$\sqrt{3}$

correct answer $= 2$

$5\%5 = 0$

$-3\%5$ $\quad (-3+5)\%5$

$\Rightarrow (-3+5)\%5 = (-3\%5) = 2\%5 = 2$

1. $a \% m = b \% m$

Ex. $-3 \% 2 \longrightarrow C++ \quad 3 \% 2 \rightarrow 2$

$\hookrightarrow -1 + m = 2$

$\therefore m =$

$\hookrightarrow (-3 + \underbrace{2 \times 2}) \% 2$

$\hookrightarrow 1 \% 2 = 1$

Ex. $-a \% b \rightarrow C++ \Rightarrow \underbrace{(-(a \% b) + m) \% m}$

Ex. $-15 \% 4 \rightarrow C++ \Rightarrow -(15 \% 4) \Rightarrow \underline{-3}$

$a \% m$

$0 \leq a \% m < m$

$-a \% m$

$-m < -a \% m \leq 0$

$\hookrightarrow (-3 + \underbrace{4}) \% m$

$\hookrightarrow \underline{1}$

$-m < 0 \leq +m$

$0 \leq \underline{m}$

1. $a \% m = b \% m$

$\Rightarrow (a-k) \% m = (b-k) \% m$

2. $a \% m = b \% m$ & $c \% m = d \% m$

$\Rightarrow (a-c) \% m = (b-d) \% m$

3. $(a-c) \% m = ((a \% m) - (k \% m)) \% m$

c is $+ve$

$+ve$

can be negative

$+ve$

$\Rightarrow (a-c) \% m = ((a \% m) + m - (c \% m)) \% m$

$-ve$

Multiplication

1. $a \equiv_m b$

   $\hookrightarrow (a \times k) \equiv_m (b \times k)$ $\forall k \in \mathbb{Z}$

2. $a \equiv_m b$ & $c \equiv_m d$

   $\hookrightarrow (a \times c) \equiv_m (b \times d)$

3. $(a \times b) \% m = ((a \% m) \times (b \% m)) \% m$

$a = \left\lfloor \frac{a}{m} \right\rfloor \times m + a \% m$

$b = \left\lfloor \frac{b}{m} \right\rfloor \times m + b \% m$

$a \times b =$

$\left\lfloor \frac{a}{m} \right\rfloor \left\lfloor \frac{b}{m} \right\rfloor m^2 + \left\lfloor \frac{a}{m} \right\rfloor \times (b \% m) \times m + \left\lfloor \frac{b}{m} \right\rfloor + (a \% m) \times m$

≥ 0 ≥ 0 ≥ 0

$+ (a \% m) \times (b \% m)$

$(a \times b) \% m = ((a \% m) \times (b \% m)) \% m$

C++ $\quad m \to 10^9+7$

$a \% m \longrightarrow [0, m-1]$

$b \% m \longrightarrow [0, m-1]$

$(10^9+7) \times (10^9+7) \approx 10^{18}$ int

long long $\leq 9 \times 10^{18}$

☆ Always use long long in modular multiplication.

Q. (18+23) %17

A. 5

B. 7

C. 6

D. 9

⇒ (18 + 23) % 17 → 41 % 17

17 × 2 = 34

↳ ((18 % 17) + (23 % 17)) % 17

↳ (1 + 6) % 17

41
- 34

7

↳ 7 % 17

↳ 7

Q. $(18-23)\%17$

A. 5

B 1

C. 12 ✓

D. 16

$(18-23)\%17 \Rightarrow -5\%17 \Rightarrow (-5+17)\%17$

$\Rightarrow 12\%17$

$\Rightarrow 12$

$-5\%17 = 12\%17$

$= 29\%17$

$= 46\%17$

$((19 \% 17) - (23 \% 17)) \% 17$

↳ $(1 - 6) \% 17$

↳ $-5 \% 17 \Rightarrow 12$

Q. $(18 \times 23) \% 17$

A. 1

B. 7

C. 6

D. 12

$(18 \times 23) \% 17$

$((18 \% 17) \times (23 \% 17)) \% 17$

$(1 \times 6) \% 17 = 6$

18×23

$\hookrightarrow 414$

$\left\lfloor \frac{414}{17} \right\rfloor$?

$\hookrightarrow 24$

$(18 \times 23) \% 17 = 18 \times 23 - \left\lfloor \frac{18 \times 23}{17} \right\rfloor \times 17$

$\Rightarrow 414 - 24 \times 17$

$\Rightarrow 6$

Factorials → $n! = 1 \times 2 \times 3 \ldots n$

- $1! = 1 = 1$
- $2! = 1 \times 2 = 2$
- $3! = 1 \times 2 \times 3 = 6$
- $4! = 1 \times 2 \times 3 \times 4 = 24$
- $5! = 1 \times 2 \times 3 \times 4 \times 5 = 120$
- $n! = (n-1)! \times n$

$100!$ % $m \rightarrow 10^{947}$

$10^5!$

$n!$

$1! \% m$

$2! \% m$

$3! \% m$

$$\hookrightarrow \quad x! \,\%\, m = \Big(\big((x-1)! \,\%\, m \big) \times \big(x \,\%\, m \big) \Big) \,\%\, m$$

$\%\, m$

Q. There is a no. x, which is

↳ $x \% 2 = 1$

↳ $x \% 3 = 2$

↳ $x \% 5 = 3$

$x \% 30$?

A. 18 ×

B. 29 ×

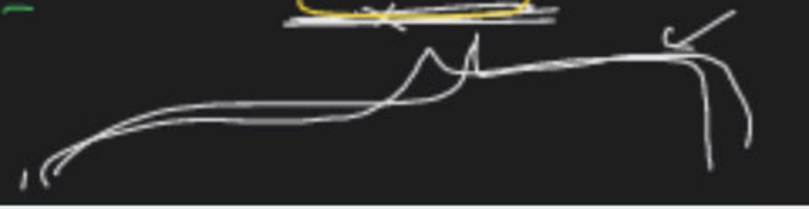
C. 23 ✓

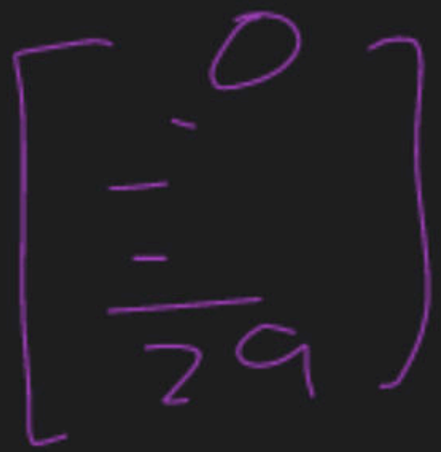
$23 \% 2 \to 1$

$23 \% 3 \to 2$

$23 \% 5 \to 3$

D. 17 ×





Chinese remainder theorem

↳ primitive root

↳ discrete log

↳ logical questions.

Tomorrow at 6 PM

Go learn CP with codechef

(y+)

Modular Exponentiation