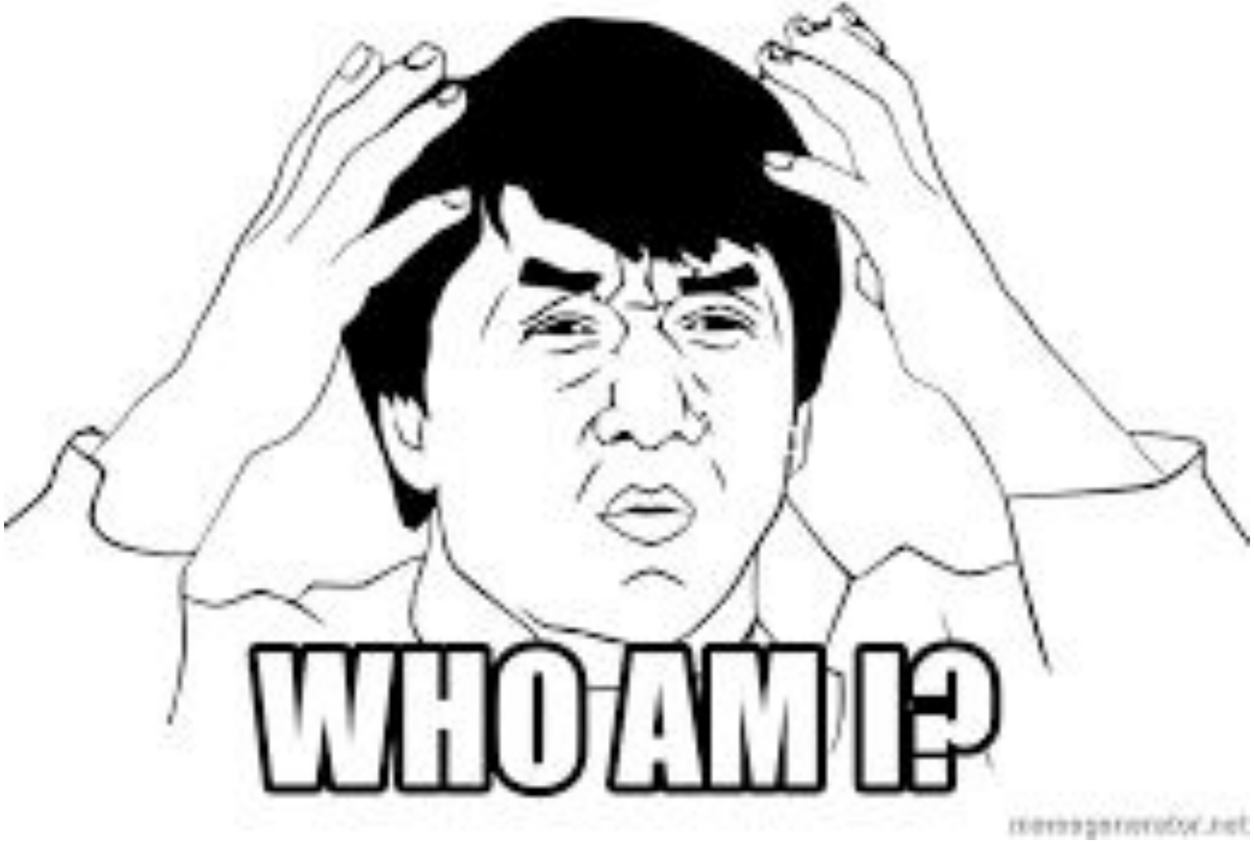
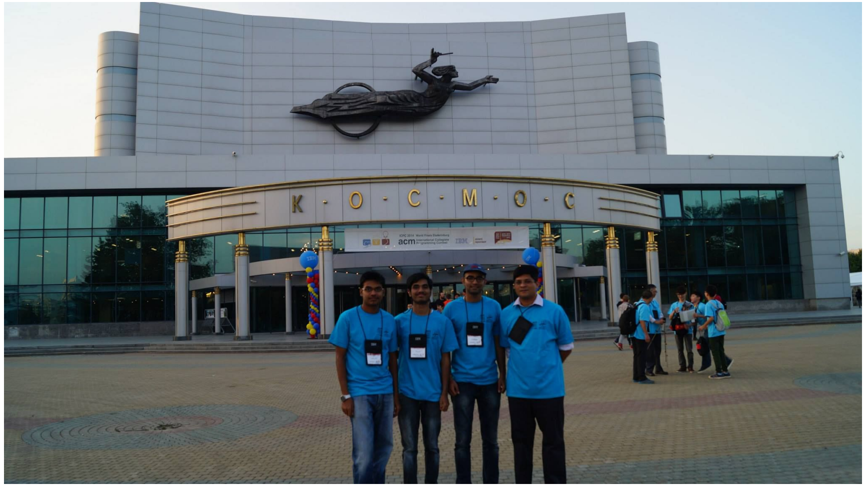
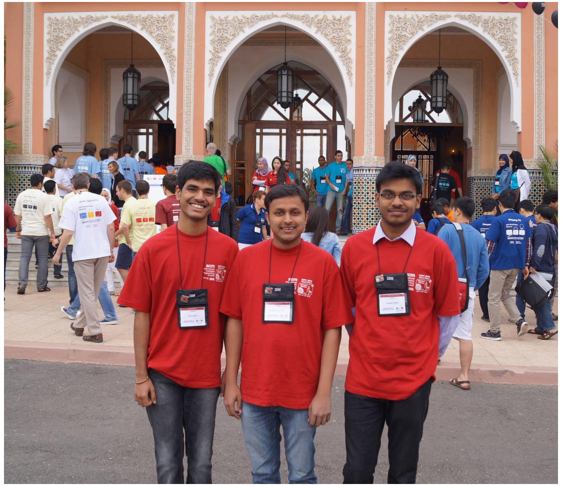
Basic/Intermediate Number Theory

-Surya Kiran Adury


WHO AM I?

ACM ICPC World Finalist (2014, 2015)

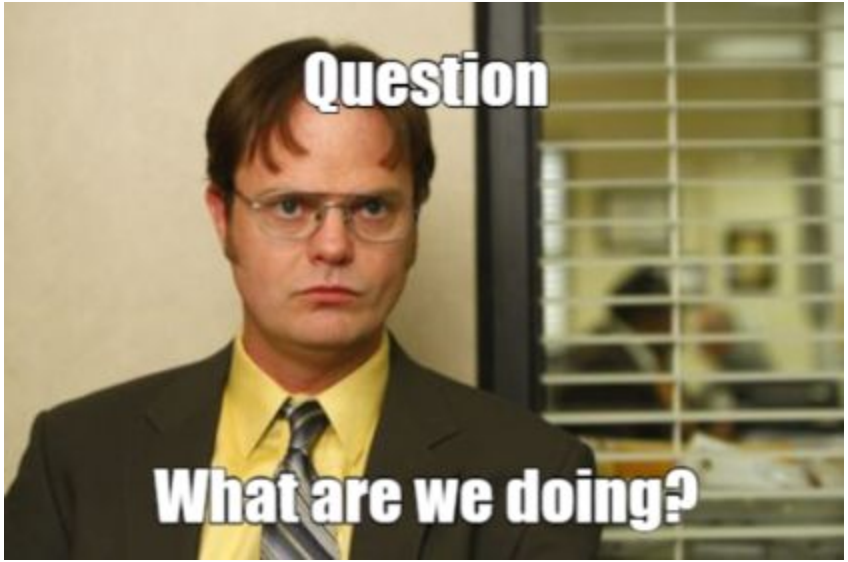




- Work Experience
  - @Google London (2015-2017)
  - @Google MTV (2017-2020)
  - Self Employed (2020-?)

- Work Experience
    - @Google London (2015-2017)
    - @Google MTV (2017-2020)
    - Self Employed (2020-?)
- Education
    - B.Tech in ECE from IIT Roorkee

- Work Experience
    - @Google London (2015-2017)
    - @Google MTV (2017-2020)
    - Self Employed (2020-?)
- Education
    - B.Tech in ECE from IIT Roorkee
- Teaching Experience
    - Weekly lectures to my juniors
    - Programming camps


Question
What are we doing?

Objective

1. Basics of modular arithmetics
2. Euclid’s theorem to find GCD of a pair of numbers
3. Bezout’s theorem, Extended Euclid’s theorem
4. Linear Diophantine Equation
5. Inverse modulo
6. Chinese remainder theorem.
7. Euler totient function
8. Fermat’s little theorem

Things to be noted in today’s class

1. We are only going to be dealing with **“integers”**.

2. We are only going to be dealing with
Addition, Multiplication, Subtraction, Division, Modular operations.

Basics of modular arithmetic

1. What is a **Modular** operation?

    a % N = ?

Basics of modular arithmetic

2. Modular representation

if $a = k * N + b$, i.e, $a \% N = b$,

then $a = b \pmod{n}$

Basics of modular arithmetic

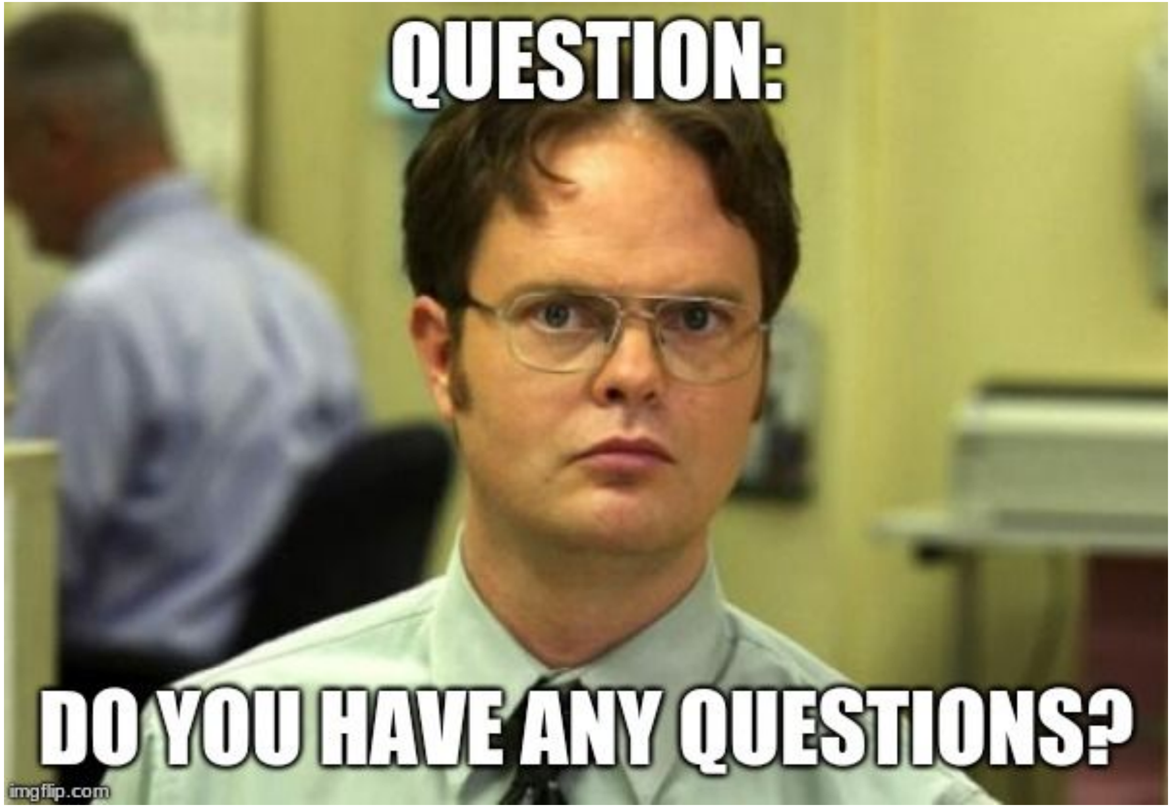
3. What are integer factors?

Basics of modular arithmetic

4. What is GCD of a pair of integers?

Basics of modular arithmetic

5. What are Co-primes?


QUESTION:
DO YOU HAVE ANY QUESTIONS?
imgflip.com

Euclid’s theorem to find GCD

Problem : Given two integers a, b. Find their GCD.

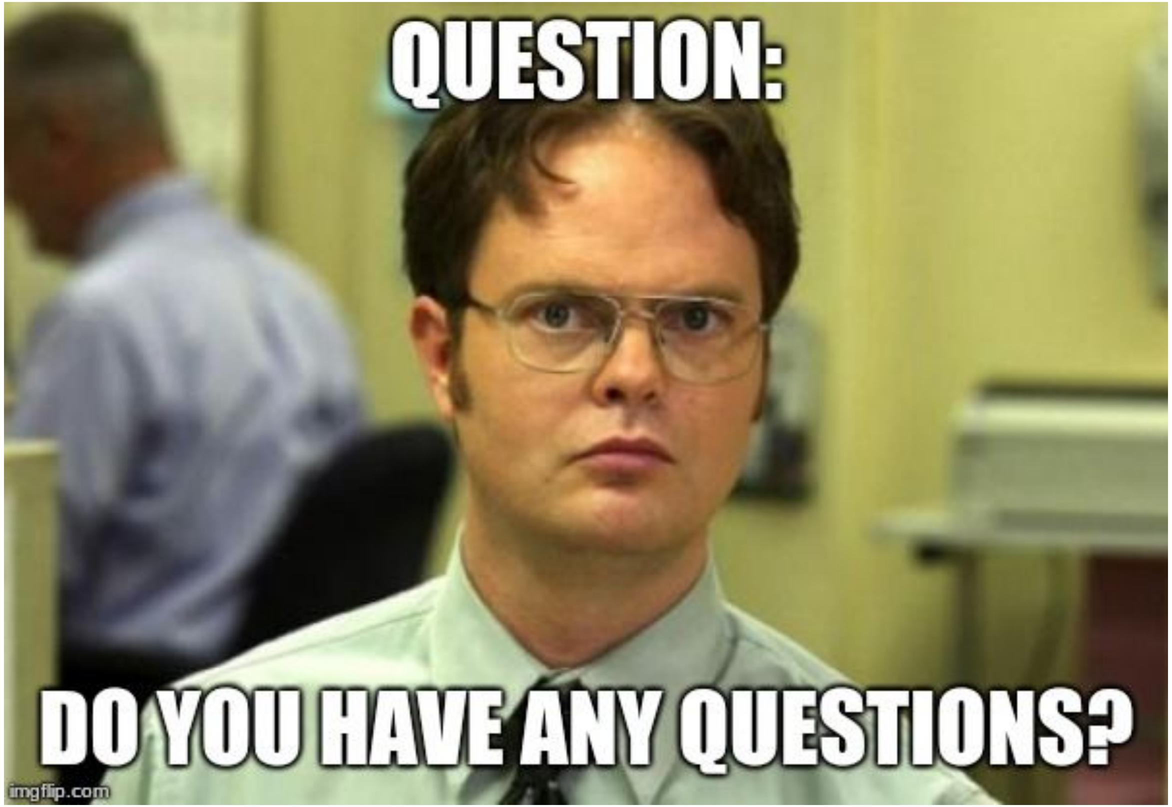
Euclid’s theorem to find GCD

Problem : Given two integers a, b. Find their GCD.

Solution :

Suppose $a < b$

$GCD(a, b) = GCD(a, b \% a)$


QUESTION:
DO YOU HAVE ANY QUESTIONS?
imgflip.com

Bezout's identity

- Let a and b be integers with greatest common divisor d.
- Then there exist integers x and y such that $ax + by = d$.

Extended Euclid’s algo

Problem : Find x, y such that $ax + by = GCD(a, b)$.

Extended Euclid's algo

Problem : Find x, y such that ax + by = GCD(a, b).

Solution :

Suppose we found the solution for the pair (b % a, a) as (x1, y1). Then we have

(b % a) * x1 + a * y1 = GCD(b % a, a)

Extended Euclid’s algo

Problem : Find x, y such that ax + by = GCD(a, b).

Solution :

Suppose we found the solution for the pair (b%a, a) as (x1, y1). Then we have

(b%a) * x1 + a * y1 = GCD(b%a, a)

Say, b = k*a + b%a

Extended Euclid's algo

Problem : Find x, y such that ax + by = GCD(a, b).

Solution :

Suppose we found the solution for the pair (b%a, a) as (x1, y1). Then we have

(b%a) * x1 + a * y1 = GCD(b%a, a)

Say, b = k*a + b%a

(b%a + k*a) * x1 + a * (y1 - k*x1) = GCD(a, b)

Extended Euclid’s algo

Problem : Find x, y such that ax + by = GCD(a, b).

Solution :

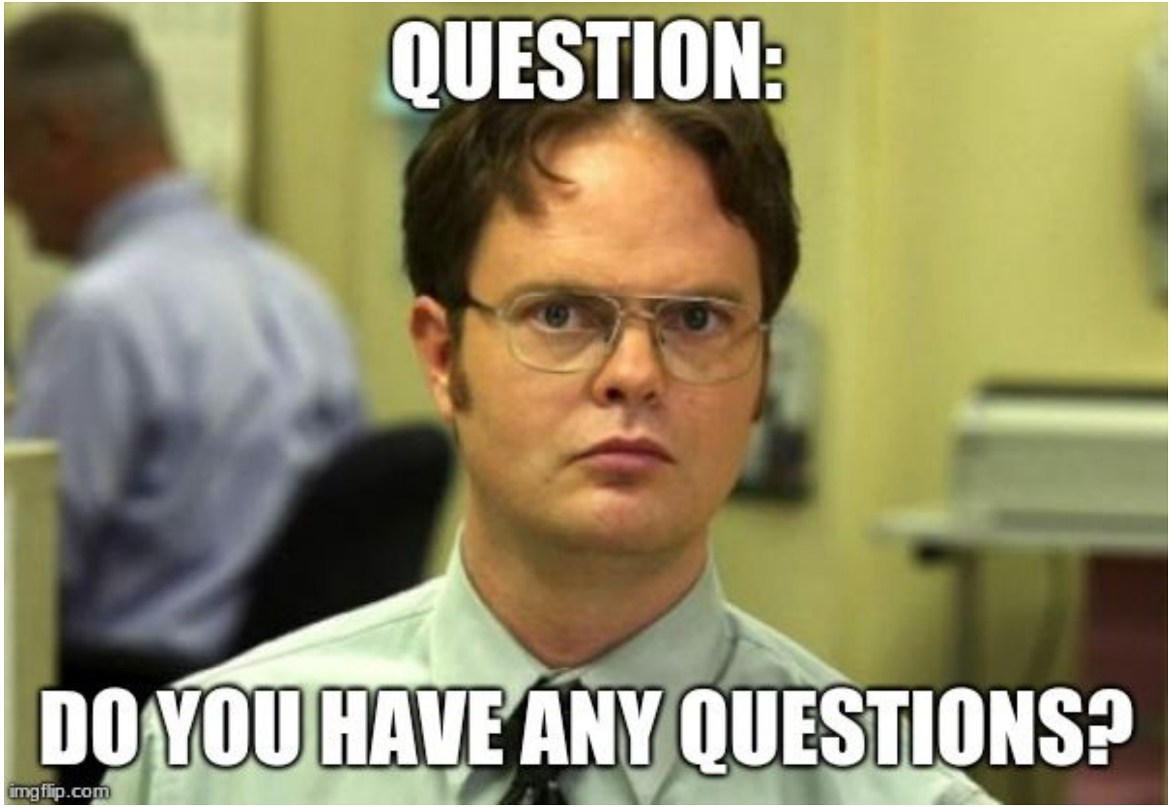
Suppose we found the solution for the pair (b%a, a) as (x1, y1). Then we have

(b%a) * x1 + a * y1 = GCD(b%a, a)

Say, b = k*a + b%a

(b%a + k*a) * x1 + a * (y1 - k*x1) = GCD(a, b)

a * x2 + b * y2 = GCD(a, b)


QUESTION:
DO YOU HAVE ANY QUESTIONS?
imgflip.com

Linear Diophantine Equations

Equations of the form $ax + by = c$

Linear Diophantine Equations

Problem: Given a, b, c. Find x, y such that $ax + by = c$

Linear Diophantine Equations

Problem: Given a, b, c. Find x, y such that $ax + by = c$

Solution: When does a solution exist?

Linear Diophantine Equations

Problem: Given a, b, c. Find x, y such that $ax + by = c$

Solution: When does a solution exist?

Only when c % GCD(a, b) == 0, why?

Linear Diophantine Equations

Problem: Given a, b, c. Find x, y such that   ax + by = c

Solution: When does a solution exist?

Only when c % GCD(a, b) == 0

Say GCD(a, b) = g, then c = d * g

Linear Diophantine Equations

Problem: Given a, b, c. Find x, y such that $ax + by = c$

Solution: When does a solution exist?

Only when c % GCD(a, b) == 0

Say GCD(a, b) = g, then c = d * g

First find ap + bq = g using extended euclid's algo.

Linear Diophantine Equations

Problem: Given a, b, c. Find x, y such that $ax + by = c$

Solution: When does a solution exist?

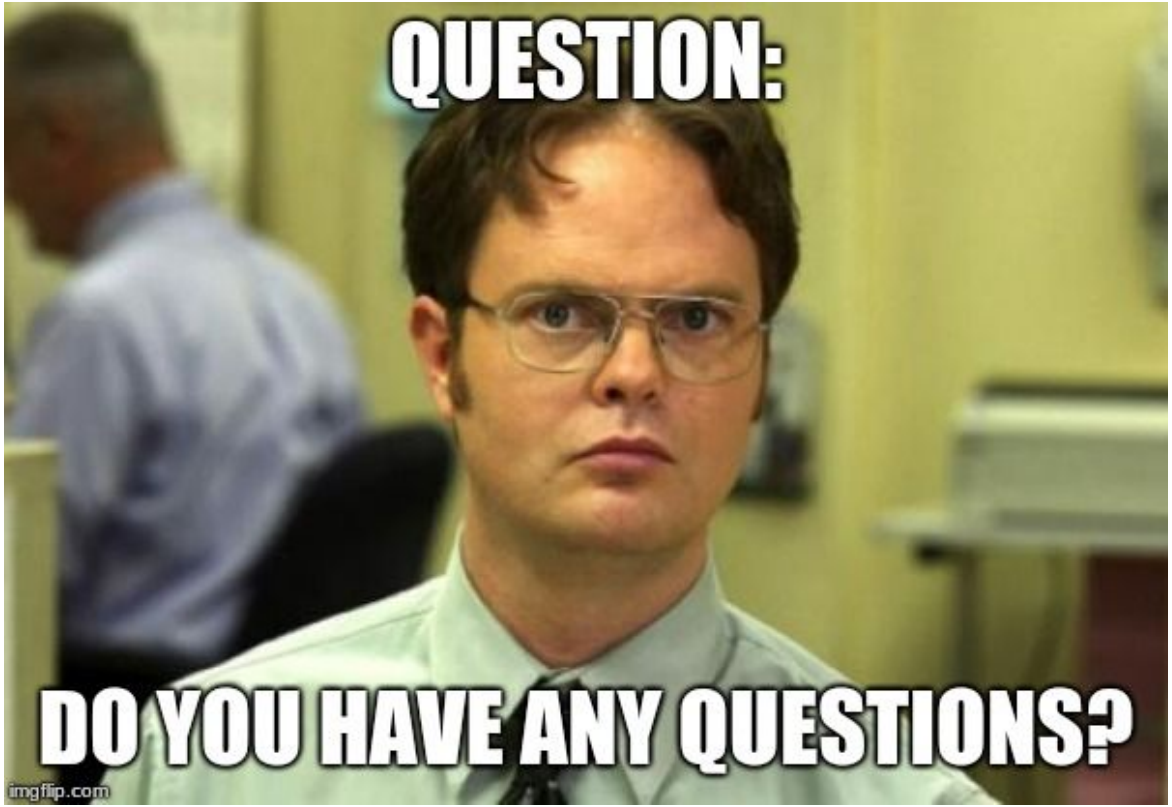
Only when c % GCD(a, b) == 0

Say GCD(a, b) = g, then $c = d * g$

First find $ap + bq = g$ using extended euclid's algo.

Then $apd + bqd = gd$,

which is same as $ax + by = c$, where $x = pd$, $y = qd$, $c = gd$.


QUESTION:
DO YOU HAVE ANY QUESTIONS?
imgflip.com

Inverse modulo

a*b = 1 (mod m)

b = a^{-1}

Inverse modulo

How to find inverse modulo?

Inverse modulo

How to find inverse modulo?

Using Extended euclid’s algorithm!

Inverse modulo

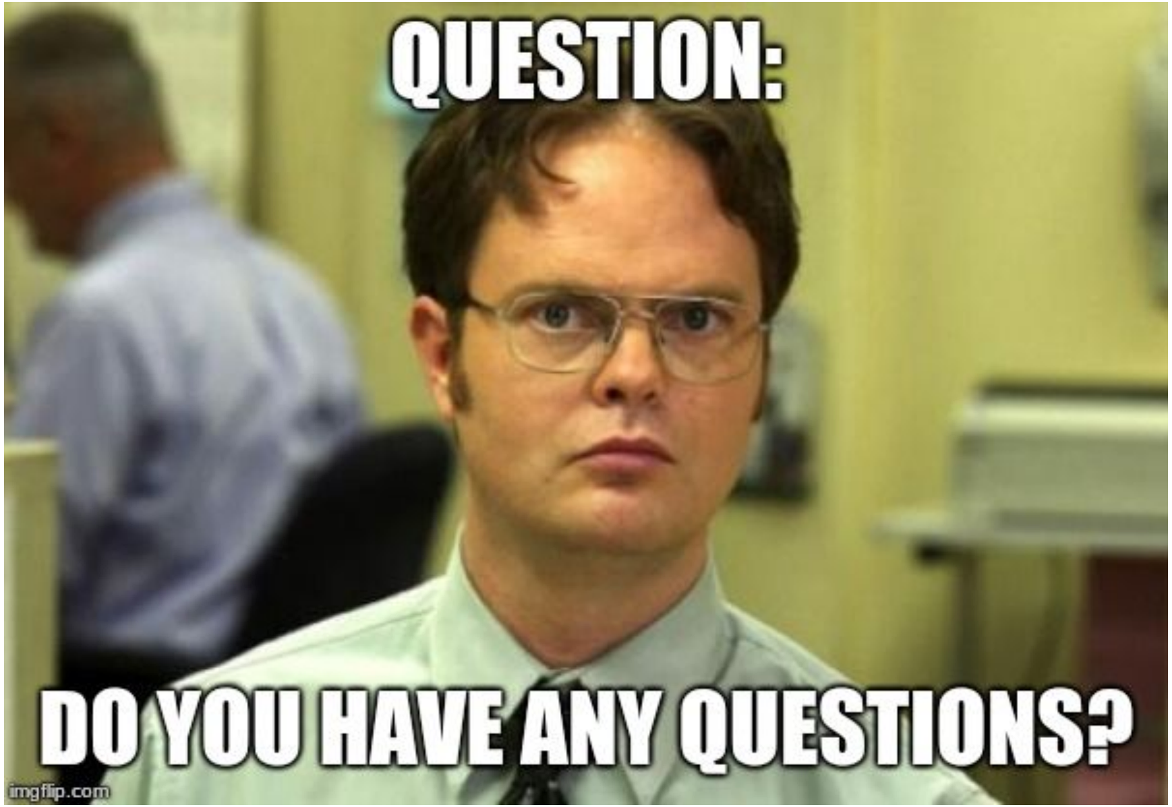
How to find inverse modulo?

Using Extended euclid’s algorithm!

Since a, m are coprime

$$a \cdot x + m \cdot y = 1.$$

$$a \cdot x \equiv 1 \pmod{m}.$$


QUESTION:
DO YOU HAVE ANY QUESTIONS?
imgflip.com

Chinese remainder theorem

- Let $n_1, ..., n_k$ be integers greater than 1. Let us denote by N the product of the n_i

- The Chinese remainder theorem asserts that if the n_i are pairwise coprime, and if $a_1, ..., a_k$ are integers such that $0 \le a_i < n_i$ for every i, then there is one and only one integer x, such that $0 \le x < N$ and $x = a_i \pmod{n_i}$ for every i.

Chinese remainder theorem

- Case of two moduli
- We want to solve the system:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2}, \end{aligned}$$

Chinese remainder theorem

- Case of two moduli
- We want to solve the system:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2}, \end{aligned}$$

$$m_1 n_1 + m_2 n_2 = 1.$$

Chinese remainder theorem

- Case of two moduli
- We want to solve the system:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2}, \end{aligned}$$

$$m_1 n_1 + m_2 n_2 = 1.$$

$$x = a_1 m_2 n_2 + a_2 m_1 n_1.$$

Chinese remainder theorem

- Case of two moduli
- We want to solve the system:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2}, \end{aligned}$$

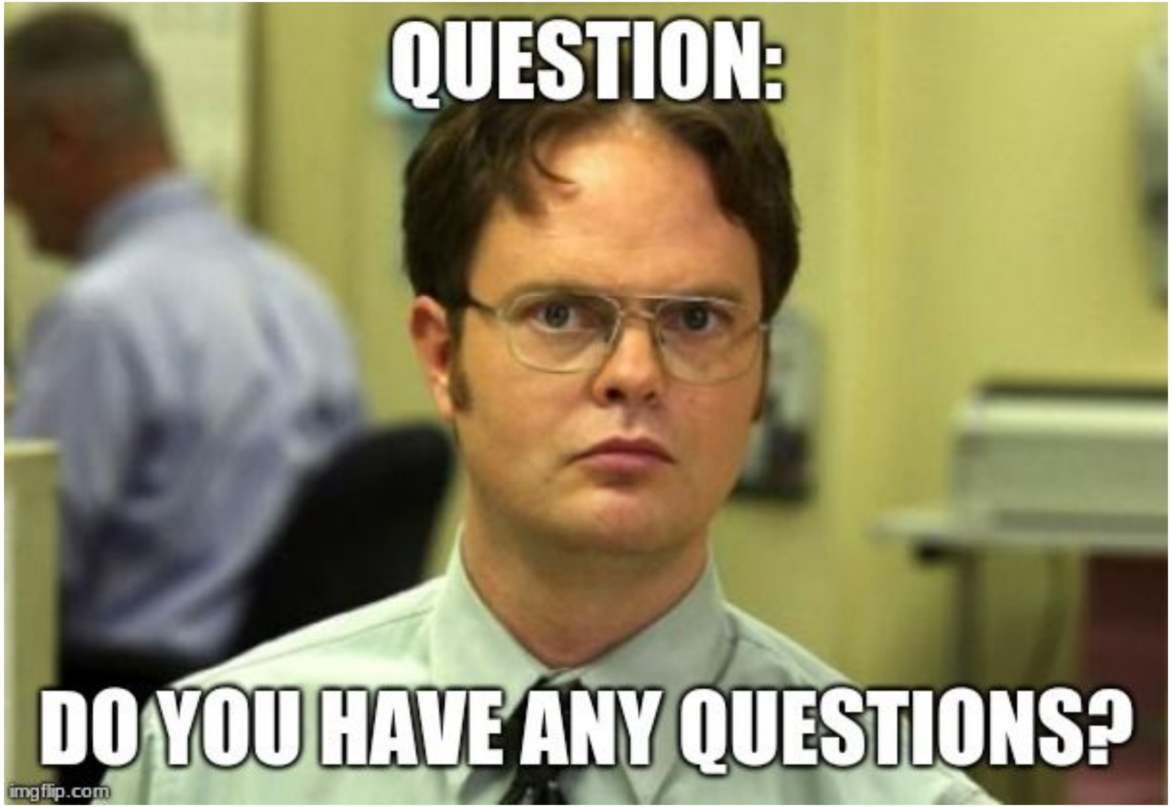
$$m_1 n_1 + m_2 n_2 = 1.$$

$$x = a_1 m_2 n_2 + a_2 m_1 n_1.$$

$$\begin{aligned} x &= a_1 m_2 n_2 + a_2 m_1 n_1 \\ &= a_1 (1 - m_1 n_1) + a_2 m_1 n_1 \\ &= a_1 + (a_2 - a_1) m_1 n_1, \end{aligned}$$

Chinese remainder theorem

- How to find for general case?


QUESTION:
DO YOU HAVE ANY QUESTIONS?
imgflip.com

Euler’s totient function $\phi(n)$

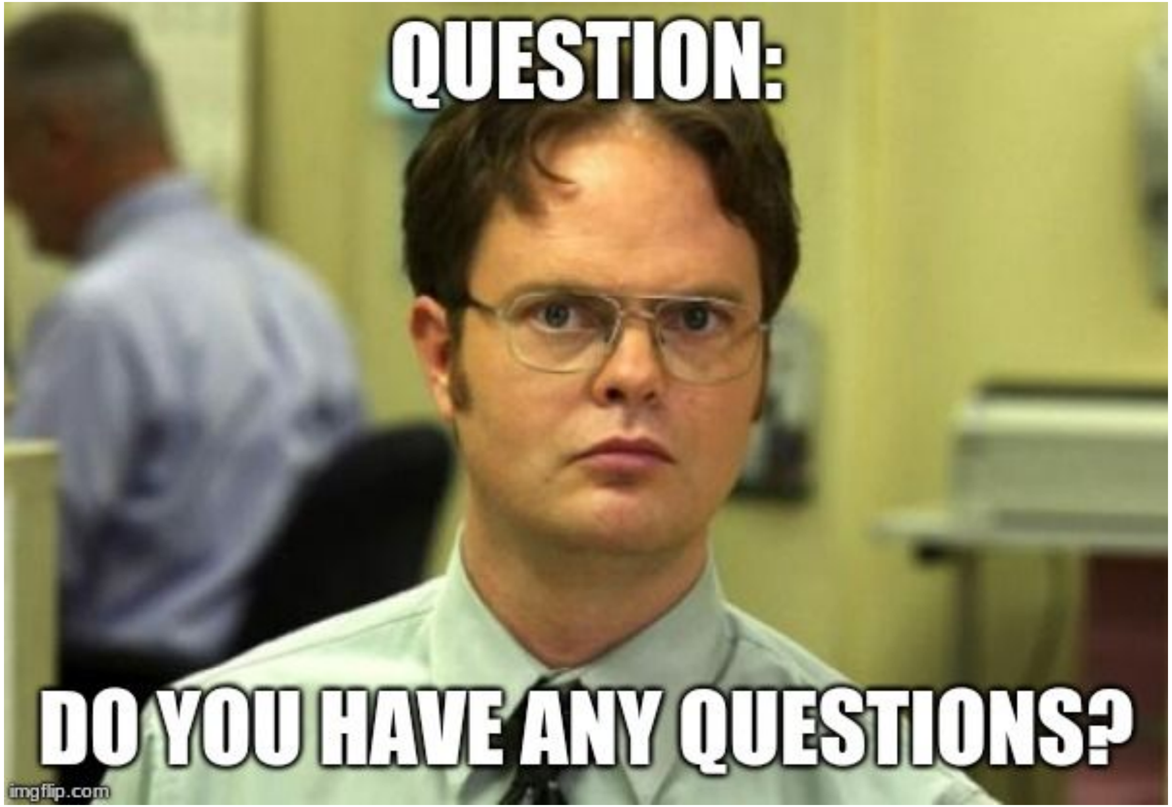
Number of numbers less than **n** which are coprime to **n.**

Euler's totient function $\phi(n)$

$$\phi(ab) = \phi(a)\phi(b)$$

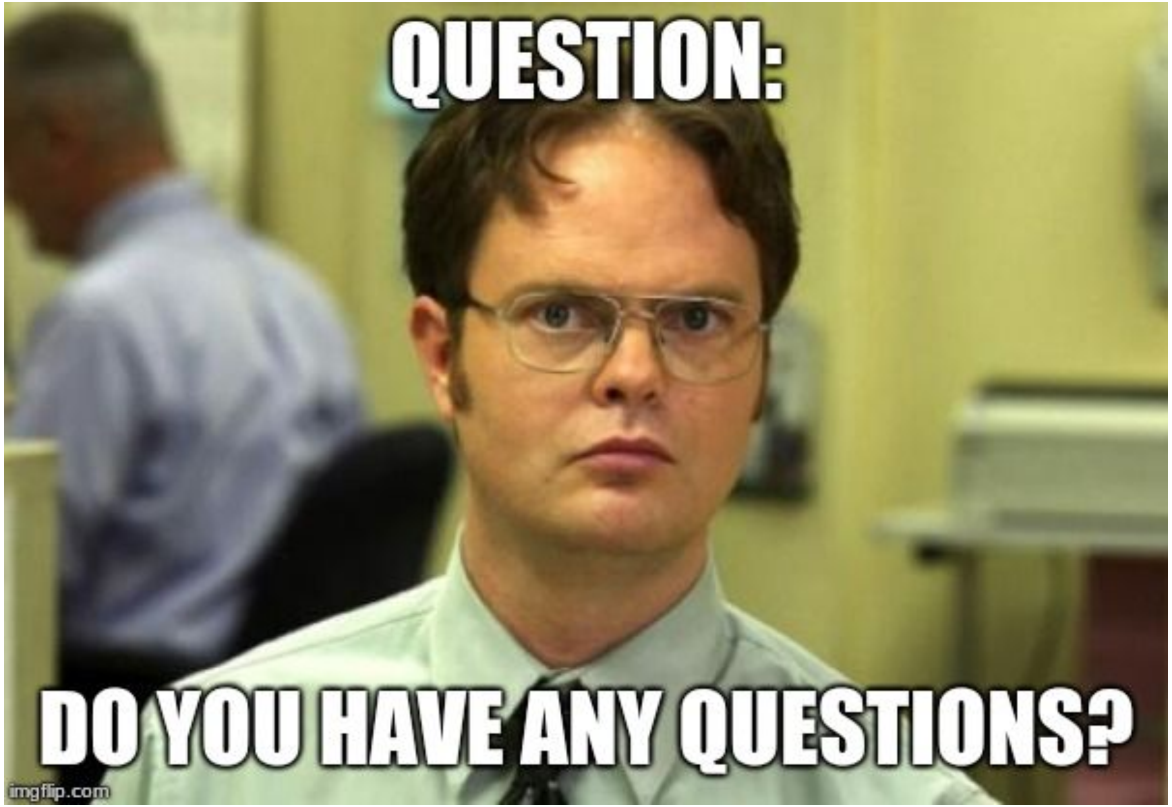
Euler’s totient function $\phi(n)$

$\phi(p) = p - 1$


QUESTION:
DO YOU HAVE ANY QUESTIONS?
imgflip.com

Fermat's little theorem

Let p be a prime which does not divide the integer a, then $a^{p-1} \equiv 1 \pmod{p}$.


QUESTION:
DO YOU HAVE ANY QUESTIONS?
imgflip.com

Resources:

a. **http://e-maxx.ru/algo/**

b. Modulus arithmetic - basic postulates [Including modular linear equations , Continued fraction and Pell's equation]
   - Suggested Reading -
     1. Chapter 1 from Number Theory for Computing by SY Yan [Recommended]
     2. 31.1, 31.3 and 31.4 from Cormen
     3. www.topcoder.com/tc?module=Static&d1=tutorials&d2=primeNumbers

c. Fermat's theorem, Euler Totient theorem (totient function, order , primitive roots)
   - Suggested Reading
     1. 1.6, 2.2 from Number Theory by SY Yan
     2. 31.6 , 31.7 from Cormen
   - Problems
     1. http://projecteuler.net/index.php?section=problems&id=70
     2. http://www.spoj.pl/problems/NDIVPHI/

d. Chinese remainder theorem
   - Suggested Reading
     1. 31.5 from Cormen
     2. 1.6 from Number Theory by SY Yan
   - Problems
     1. Project Euler 271
     2. http://www.topcoder.com/stat?c=problem_statement&pm=10551&rd=13903

e. GCD using euclidean method
   - Suggested Reading
     1. 31.2 Cormen
   - Problems -
     1. GCD on SPOJ
     2. http://uva.onlinejudge.org/external/114/11424.html

Problem - NDIVPHI on Spoj

NDIVPHI - N DIV PHI_N

#math #number-theory

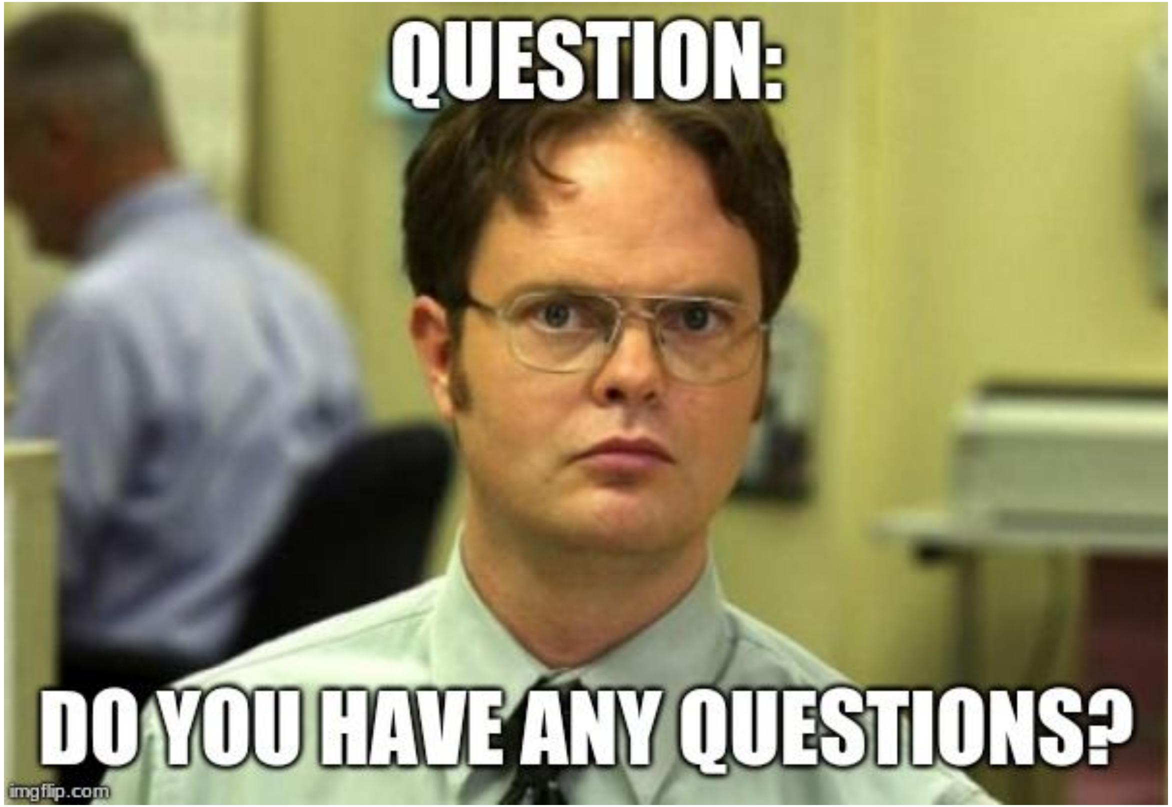
Given an integer $N <= 10^{40}$ find the smallest $m <= N$ such that $m/phi(m)$ is maximum.

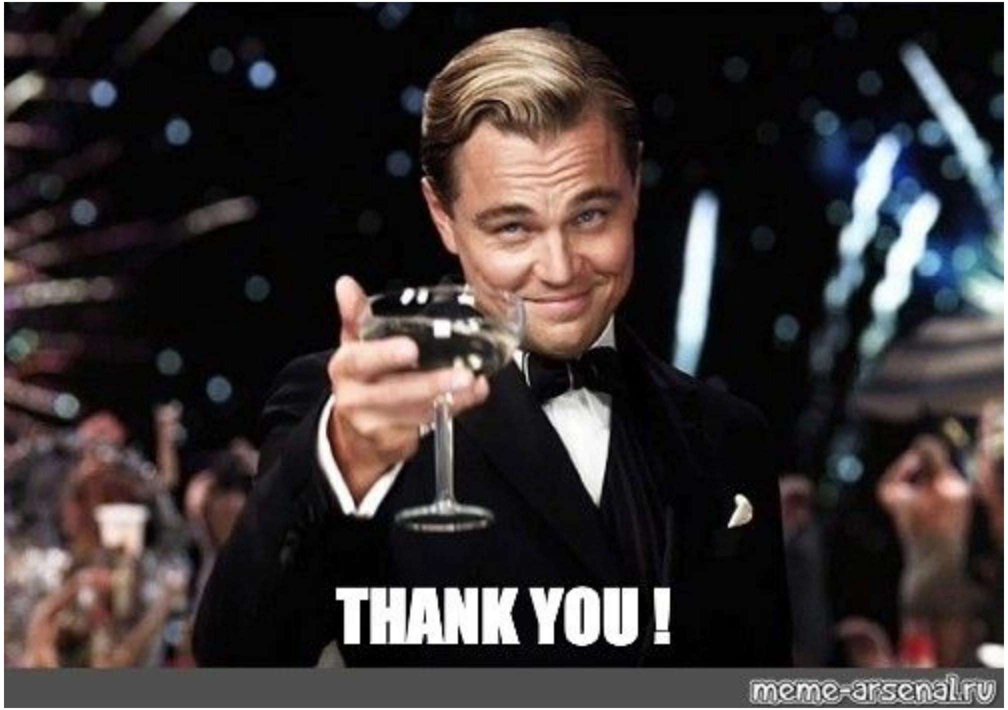
Input

N_1
N_2
.
.
.
N_{20}

Output

m_1
m_2
.
.
.
m_{20}


QUESTION:
DO YOU HAVE ANY QUESTIONS?
imgflip.com


THANK YOU !
meme-arsenal.ru