Rohit and Ayush Tutorial

Pre-requisites:

This problem will concepts of euclidean algorithm, gcd and divisibility to solve. Make sure your basics of gcd, euclidean algorithm and number theory are clear before attempting this problem. The following links can help you learn the prerequisites:

- https://www.topcoder.com/community/data-science/data-science-tutorials/prime-numbers-factorization-and-euler-function/
- https://www.topcoder.com/community/data-science/data-science-tutorials/mathematics-for-topcoders/
- http://www.geeksforgeeks.org/basic-and-extended-euclidean-algorithms/
- http://www.virtualnerd.com/pre-algebra/factors-fractions-exponents/prime-factorization-greatest-common-factor/greatest-common-factor/greatest-common-factor-two-numbers

Problem Description:

In this problem, we have to find the gcd of two mersenne numbers M_n and M_m .
A mersenne number M_a is given by:
$M_a = 2^a - 1$
Now, as per the constraints, $0 \le n, m \le 10^3$. This makes it infeasible to calculate the gcd of two numbers as large as $2^{\wedge}10^3$. Moreover, we have to calculate the gcd of 'N' such pairs where $1 \le N \le 10^5$. The challenge is to calculate the gcd of so many large numbers in practical time.

Difficulty Level:

Hard

Editorial:

We have to compute the gcd of $2^m - 1$ and $2^n - 1$. We cannot compute it directly and can use a simple concept of number theory to make it possible:

Theorem:

$\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1$

Proof:

Let $m \ge n \ge 1$

Applying Euclidean Algorithm,
$\gcd(a^m-1, a^n-1) = \gcd(a^n(a^{m-n}-1), a^n-1)$
$\Rightarrow \gcd(a^m-1, a^n-1) = \gcd(a^n(a^{m-n}-1), a^n-1)$.
$\Rightarrow \gcd(a^m-a^n, a^n-1)$

Iterate this until it becomes
$\gcd(a^{\gcd(m,n)}-1, a^{\gcd(m,n)}-1) = a^{\gcd(m,n)}-1$

More generally,

if $\gcd(a,b)=1$, $a,b,m,n \in Z^+$, $a \geq b$, then

$$\gcd(a^m-b^m, a^n-b^n) = a^{\gcd(m,n)} - b^{\gcd(m,n)}$$

Proof:

Since $\gcd(a,b)=1$, we get $\gcd(b,d)=1$, so $b^{-1} \pmod d$ exists.

$$D \mid a^m-b^m, a^n-b^n \Leftrightarrow (ab^{-1})^m \equiv (ab^{-1})^n \equiv 1 \pmod d$$

$$d \mid am-bm, an-bn \Leftrightarrow (ab-1)m \equiv (ab-1)n \equiv 1(modd)$$

$$\Leftrightarrow ord_d(ab^{-1}) \mid m,n \Leftrightarrow ord_d(ab^{-1}) \mid \gcd(m,n)$$

$$\Leftrightarrow ord_d(ab^{-1}) \mid m,n \Leftrightarrow ord_d(ab^{-1}) \mid \gcd(m,n)$$

$$\Leftrightarrow (ab^{-1})^{\gcd(m,n)} \equiv 1 \pmod d \Leftrightarrow a^{\gcd(m,n)} \equiv b^{\gcd(m,n)} \pmod d$$

Complexity of solution:

The complexity of the solution will be the same as that of finding gcd of two numbers using euclidean algorithm. Which is: O(Log min(a, b)). Here, a and b are the two numbers whose gcd is to be calculated.