Number Theory

By Hasan Murad

Lecturer,

CSE,UAP

Definition

$$m \backslash n \iff m > 0 \text{ and } n = mk \text{ for some integer } k$$

$$\gcd(m, n) = \max\{k \mid k \backslash m \text{ and } k \backslash n\}$$

$$\operatorname{lcm}(m, n) = \min\{k \mid k > 0, \quad m \backslash k \text{ and } n \backslash k\}$$

Euclid's algorithm

- A 2300-year-old method

$$\gcd(0, n) = n;$$
$$\gcd(m, n) = \gcd(n \bmod m,\ m)$$

$$\gcd(12, 18) = \gcd(6, 12) = \gcd(0, 6) = 6$$

PRIME EXAMPLES

- How many primes are there?
- A lot.
- In fact, infinitely many.
- Euclid proved this long ago.
- Suppose there were only finitely many primes, say k of them - 2, 3, 5, …. , Pk. Then, said Euclid, we should consider the number

$$M = 2 \cdot 3 \cdot 5 \cdot \ldots \cdot P_k + 1$$

$$2^p - 1$$

(where p is prime, as always in this chapter) are called *Mersenne numbers*, after Father Marin Mersenne who investigated some of their properties in the seventeenth century [269]. . The Mersenne primes known to date occur for $p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203,$ 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, and 756839.

The number $2^n - 1$ can't possibly be prime if n is composite, because $2^{km} - 1$ has $2^m - 1$ as a factor:

$$2^{km} - 1 = (2^m - 1)(2^{m(k-1)} + 2^{m(k-2)} + \cdots + 1).$$