Number Theory

Primes: A positive integer p is called *prime* if it has just two divisors, namely 1 and p. By convention, 1 is not prime, so the sequence of primes starts out like this:
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,⋯
Primes are of great importance, because they are the fundamental building blocks of all the positive integers. Any positive integer n can be written as a product of primes,

$$n = p_1 p_2 \cdots p_m = \prod_{k=1}^{m} p_k \quad \text{,where } p_1 \le p_2 \le \cdots \le p_m \quad \cdots \quad (1)$$

for prime integers:
11 = 1 * 11
43 = 1 * 43

For example, $12 = 2 \cdot 2 \cdot 3$; $11011 = 7 \cdot 11 \cdot 11 \cdot 13$; $11111 = 41 \cdot 271$
Here the products denoted by $\prod$ are analogous to sums denoted by $\sum$. There is only one way to write n as a product of primes in non-decreasing order. This statement is called the Fundamental Theorem of Arithmetic.

We can prove the Fundamental Theorem of Arithmetic by contradiction. Suppose, we have two factorization of an integer number, n

$$n = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n \quad , \; p_1 \le p_2 \le \cdots \le p_m \text{ and } q_1 \le q_2 \le \cdots \le q_n$$

where p's and q's are all prime. We will prove that $p_1 = q_1$. If not, we can assume that $p_1 < q_1$, making p_1 smaller than all q's. Since p_1 and q_1 are prime their gcd must be 1. Hence, Euclid's self-certifying algorithm gives us integer a and b such that

$$ap_1 + bq_1 = 1$$

GCD (p1, q1) = 1 because both p1, q1 primes
Euclid's theorem: The GCD of two numbers can always be written as a linear combination of the two numbers ==> so, $ap_1 + bq_1 = 1$ for integers a, b

****
MUST SEE THIS PROOF
****

$$\Rightarrow ap_1 q_2 q_3 \cdots q_n + bq_1 q_2 q_3 \cdots q_n = q_2 q_3 \cdots q_n$$
$$\Rightarrow ap_1 q_2 q_3 \cdots q_n + bn = q_2 q_3 \cdots q_n$$
$$\Rightarrow ap_1 q_2 q_3 \cdots q_n + bp_1 p_2 p_3 \cdots p_m = q_2 q_3 \cdots q_n$$
$$\Rightarrow p_1 (aq_2 q_3 \cdots q_n + bp_2 p_3 \cdots p_m) = q_2 q_3 \cdots q_n$$

p1 can't divide ...

Since p_1 divides left hand side, hence p_1 should divide right hand side $q_2 q_3 \cdots q_n$. But p_1 is ~~not divisible by~~ $q_2 q_3 \cdots q_n$ according to our assumption. Thus p_1 and q_1 must be equal. Similarly we can show that, $p_2 = q_2$, $p_3 = q_3$, ⋯ , $p_m = q_n$.

Every positive integer can be written uniquely in the form

$$n = \prod_{p} p^{n_p} \text{ where each } n_p \ge 0 \quad \cdots \quad (2)$$

example:
100 = 2^2 * 3^0 * 5^2 * 7^0 * 11^0 * ...
352 = 2^5 * 3^0 * 5^0 * 7^0 * 11^1 * ...

np is the power of the prime p in the unique prime factorization of the integer n

Formula (2) represents n uniquely, so we can think of the sequence $(n_2, n_3, n_5, \cdots)$ as a *number system* for positive integers. For example, prime exponent representation of 12 is (2 , 1 , 0 , 0 , . . .) and the prime exponent representation of 18 is (1 , 2 , 0 , 0 , . . .). To multiply two number, we simply add their representations. In other words,

$$k = mn \quad \Leftrightarrow \quad k_p = m_p + n_p \quad \text{for all } p \quad \cdots \quad (3)$$

This implies that

$$m \backslash n \quad \Leftrightarrow \quad m_p \le n_p \quad \text{for all } p \quad \cdots \quad (4)$$

and it follows immediately that,

Q: Write the Prime Exponent Representation of GCD(m,n), LCM(m,n) and PRODUCT(m,n). Also, Provide Concrete Numeric Example.

$$k = \gcd(m,n) \Leftrightarrow k_p = \min(m_p, n_p) \quad \text{for all } p \quad \cdots \quad (5)$$

$$k = lcm(m,n) \Leftrightarrow k_p = \max(m_p, n_p) \quad \text{for all } p \quad \cdots \quad (6)$$

For example, since $12 = 2^2 \cdot 3^1$ and $18 = 2^1 \cdot 3^2$, we can get their gcd and lcm by taking the min and max of common exponents:

$\gcd(12,18) = 2^{\min(2,1)} \cdot 3^{\min(1,2)} = 2^1 \cdot 3^1 = 6$

$lcm(12,18) = 2^{\max(2,1)} \cdot 3^{\max(1,2)} = 2^2 \cdot 3^2 = 36$

Q: What do you understand by Euclid number/ Mersenne number? Explain with Concrete examples.

Prime Examples: Euclid proved that, there are infinitely many primes. The proof is as follows: Suppose, there are only finitely many primes, say k of them $2,3,5,\cdots,p_k$. Then we should consider the number, $M = 2 \cdot 3 \cdot 5 \cdot \cdots \cdot p_k + 1$.

None of *k* primes can divide *M*, because each divides *M*-1. Thus there must be some other prime that divides *M*; perhaps *M* itself is a prime. This contradicts our assumption that, $2,3,5,\cdots,p_k$ are the only primes, so there must be infinitely many prime.

$e_0 = 1$ and $e_1 = 1+1 = 2$ .... now compute e2, e3, e4, so on ...

Euclid Number: $e_n = e_1 e_2 \cdots e_{n-1} + 1$, when $n \geq 1$ $\cdots$ (7)

The sequence starts out

$e_1 = 1+1 = 2$

$e_2 = 2+1 = 3$

$e_3 = 2 \cdot 3 + 1 = 7$

$e_4 = 2 \cdot 3 \cdot 7 + 1 = 43$

en = e0 * e1 * e2 * ... ... en-1 + 1

e2 = 1.2 + 1 = 3

e3 = 1.2.3 + 1 = 7

e4 = 1.2.3.7 + 1 = 43 **e5 = 1.2.3.7.43 + 1 = 1807**

these are all prime. But the next case, e_5 is $1807 = 13 \cdot 139$. However, Euclid numbers are all *relatively prime* to each other; that is

$\gcd(e_m, e_n) = \gcd(1, e_m) = \gcd(0,1) = 1$, where $m \neq n$.

Recurrence (7) can be simplified by removing three dots. If $n > 1$, we have

$e_n = e_1 e_2 \cdots e_{n-2} e_{n-1} + 1 = (e_{n-1} - 1) e_{n-1} + 1 = e_{n-1}^2 - e_{n-1} + 1$

The numbers of the form $2^p - 1$ (where p is a prime) is called *Mersenne numbers*. The Mersenne prime known 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, 132049,216091,756839 and 859433. The number $2^n - 1$ cannot possibly prime if n is not prime, because $2^{km} - 1$ has $2^m - 1$ as a factor. We can prove it by following way:

$$1 + 2^m + 2^{2m} + 2^{3m} + \cdots + 2^{(k-1)m} = \frac{2^{km} - 1}{2^m - 1}$$

Left hand side of the equation is integer, which refers to right hand side is also an integer. That means, $2^{km} - 1$ is divisible by $2^m - 1$. Thus $2^{km} - 1$ is not a prime number.

But, $2^p - 1$ is not always a prime when p is prime. For example, $2^{11} - 1 = 2047 = 23 \cdot 89$ is the smallest such nonprime.

Short Q: Prove or Disprove that Euclid number is always Prime: Ans: Disprove by a counter example (e5 = 1807 = 13*139)

Short Q: Prove or Disprove that Mersenne number is always Prime: Ans: Disprove by Counter example (p=11 => 2^11 - 1 = 2047 = 23 *89)

Prove that: Any integer of the form 2^p - 1 can never be a prime number, given that p is a composite number.