All About Primes

Alston Yam

“Choices are made in brief seconds and paid for in the time that remains.”

—*Paolo Giordano, The Solitude of Prime Numbers*

1 Introduction

Prime numbers present an interesting field of study in number theory. In this lecture we will explore some unique properties of primes and also some applications of them in the context of mathematical competitions.

2 Prime Numbers

Definition 2.1 – Prime Number A **prime** number is a natural number that only has two distinct positive divisors.

We will define a **composite** number as a natural number that has more than two positive divisors.

Exercise 2.1 Is 1 a prime number? Justify your answer.

As we will soon see, primes are the “building blocks” of the natural numbers, and understanding them will give you a great grasp on number theory.

Lets begin with a classic yet important result on the prime numbers.

Theorem 2.1 – Euclid’s Theorem Prove that there are infinitely many prime numbers.

Proof. Assume that there are only finitely many prime numbers, say $\{p_1, p_2, \ldots, p_n\}$. Consider the number

$$N = p_1 p_2 \cdots p_n + 1$$

By construction, N is not divisible by any of the primes $p_1, p_2, \ldots, p_n$, since dividing N by any of these primes leaves a remainder of 1. Therefore, either N is prime itself or it has a prime factor that is not in our original list. In either case, we have found a prime number that is not in our original list, contradicting the assumption that there are only finitely many primes. Thus, there must be infinitely many prime numbers. □

This seems logical, however the above proof is not rigorous. To actually complete the proof, we will need to invoke the following theorem:

2.1 Fundamental Theorem of Arithmetic

Theorem 2.2 – Fundamental Theorem of Arithmetic Every integer greater than 1 can be **uniquely** expressed as a product of prime numbers, up to the order of the factors.

That is to say, every integer $n > 1$ has a unique representation of the form

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

This will allow us to complete the proof of Theorem 2.1. Specifically, only when we use this theorem can we say that N is able to be "split" into prime factors, leading to us to find our desired prime that is not in the set $\{p_1, p_2, \ldots, p_n\}$.

Exercise 2.2 Find the prime factorisation of 91.

Problem solving tip: When you encounter a problem involving integers, it's always a good idea to consider the prime factors of that number! Sometimes considering the biggest/smallest prime divisors of that number gives unexpected results that we can liase.

3 GCD and LCM

We will now move on to some more useful applications of prime numbers, and this section will be dedicated to finding the GCD and the LCM of two integers a and b. Lets first denote the prime factorisation of a and b as follows:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$
$$b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$$

where p_i are the prime factors of a and b, and α_i, β_i are the respective powers of these primes in the factorisations of a and b (Notice that some of α_i and β_i are possibly equal to 0).

Definition 3.1 – GCD and LCM The **greatest common divisor** (GCD) of a and b, denoted $\gcd(a, b)$, is defined as:

$$\gcd(a, b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_k^{\min(\alpha_k,\beta_k)}$$

The **least common multiple** (LCM) of a and b, denoted $\operatorname{lcm}(a, b)$, is defined as:

$$\operatorname{lcm}(a, b) = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \cdots p_k^{\max(\alpha_k,\beta_k)}$$

Example 3.1 For any two positive integers a and b, we have

$$ab = \operatorname{lcm}(a, b) \gcd(a, b)$$

Proof. This follows directly from the definitions of GCD and LCM.

$$\begin{aligned} ab &= p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} \cdots p_k^{\alpha_k+\beta_k} \\ &= p_1^{\max(\alpha_1,\beta_1)+\min(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)+\min(\alpha_2,\beta_2)} \cdots p_k^{\max(\alpha_k,\beta_k)+\min(\alpha_k,\beta_k)} \\ &= \operatorname{lcm}(a, b) \gcd(a, b) \end{aligned}$$

□

4 Euler's Totient Function

Definition 4.1 – Euler's Totient Function We define the function $\varphi(n)$ to be the number of positive integers less than n that are coprime to n.

This function also has a formula:

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

Where $p_1, p_2, \ldots, p_k$ are the distinct prime factors of n.

To arrive at this formula, we will need the following lemma, which we state without proof.

Theorem 4.1 – Multiplicity of Euler's Totient Function If a and b are coprime integers, then

$$\varphi(ab) = \varphi(a) \cdot \varphi(b)$$

We also have the following interesting property of the Totient Function.

Theorem 4.2 – Gauss

$$\sum_{d|n} \varphi(d) = n$$

5 Problems

Problem 5.1 If $p < q$ are two consecutive odd prime numbers, show that $p + q$ has at least 3 (not necessarily distinct) prime factors.

Problem 5.2 Find all positive integers n such that $3n - 4$, $4n - 5$, $5n - 3$ are all prime numbers.

Problem 5.3 Prove Theorem 4.1 and Theorem 4.2.

Problem 5.4 – IMO 1959/1 Prove that for any natural number n, the fraction $\frac{21n+4}{14n+3}$ is irreducible.

Problem 5.5 – NZMO 2023 Do there exist infinitely many triples (p, q, r) of positive integers with $p > q > r > 1$ such that the product

$$p! \cdot q! \cdot r!$$

is a perfect square?