Fundamental Theorem of Algebra

Dave Neary

January 15, 2021

1 Introduction

We will talk about some of the number systems you will come across, and work up to the Fundamental Theorem of Arithmetic: that positive whole numbers have a unique representation as the product of prime numbers.

2 Number systems

There are several number systems that we will come across in number theory. You might say that mathematics is a journey, inventing new number systems and abstractions to allow us to solve new types of problems we could not with the tools available before.

We start with the natural numbers $\mathbb{N} = \{1, 2, 3, \cdots\}$, or the natural numbers including 0 $\mathbb{N}_0 = \{0, 1, 2, \cdots\}$ - this is the foundation of mathematics, counting objects. The natural numbers are closed under the operations addition and multiplication, but not under subtraction. In general, we cannot find $a - b \in \mathbb{N}$ for $a, b \in \mathbb{N}$.

To enable closure under subtraction, we can extend the natural numbers to include negative numbers to produce the integers

$$\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$$

This number system is closed under addition, multiplication, **and** subtraction, but still has a limitation under division. When we try to divide a whole number into parts, we cannot do this in the integers.

To enable closure under division, we can extend the integers to include the rational numbers - fractions:

$$\mathbb{Q} = \{\frac{a}{b} | a, b \in \mathbb{Z}, b \neq 0\}$$

Finally, for now, we can extend the rational numbers to include numbers which cannot be represented by a fraction, but which can be measured on the number line, to the real numbers $\mathbb{R}$, which are essentially the rational numbers with the gaps filled in. We call a number which is in the real numbers, but is not a rational number, an irrational number.

The irrational numbers can also be subdivided into two groups. The algebraic numbers are a superset of the rational numbers which includes all exact solutions of polynomial equations with rational coefficients. This group includes all the square roots, cube roots, and in general the nth roots, and any combination of them (for example, $\sqrt[3]{7+\sqrt{13}}$ is an algebraic number).

Any number which is not the solution to any such polynomial is called a transcendental number. Well known numbers like π and e are transcendental numbers.

For now, we will focus mostly on the characteristics of the natural numbers and the integers. There will be plento of opportunity in the future to get into the other number systems - and to discover others!

3 The Fundamental Theorem of Arithmetic

Natural numbers can be grouped into different subsets. For example, we learn early in school that the numbers 2,4,6,8,... are special - they are all whole number multiples of 2, and we call them the even numbers. If a number is not even, it is odd.

There is nothing special about 2 though - we can find the set of nultiples of 3, and can even define it in general as $S = \{3, 6, 9, \cdots\} = \{3n | n \in \mathbb{N}\}$ - that is, the set contains all of the numbers which can be expressed as $3k$ for some $k \in \mathbb{N}$. We will often use this type of set definition short-hand.

Every natural number has natural number divisors. Some numbers can only be divided in natural numbers by themselves and 1. We call these numbers **prime numbers**. The first few prime numbers are 2, 3, 5, 7, 11, 13, 17. A natural number which is not a prime number is called a composite number, which means that we can write the number $n = a \cdot b$ for $a, b > 1 \in \mathbb{N}$. 4, 6, 8, 9 are the first composite numbers.

The number 1 is special - it is neither prime nor composite, by convention (which means, it's just useful to think of it as being neither - people have fought about that stuff in the past). Next, we will bring these threads together to state the Fundamental Theorem of Algebra. It is very powerful, and almost completely obvious.

Theorem 1 (The Fundamental Theorem of Arithmetic) *Every number* $n \in \mathbb{N}$ *can be expressed as a* ***unique*** *product of primes. We can write* $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ *for some set of primes* $\{p_i\}$ *and exponents* $\{\alpha_i\} \in \mathbb{N}$*.*

Starting from just this theorem, we can already prove some nice results.

3.1 Problems

Q. 1 *Prove that* $\sqrt{5}$ *is irrational.*

Proof: We will use proof by contradiction. Assume that $\sqrt{5}$ is rational, that is, that there exist $a, b \in \mathbb{N}$ such that $\gcd(a, b) = 1$ and $\sqrt{5} = \frac{a}{b}$.

Then since:

$$5 = \frac{a^2}{b^2} \implies a^2 = 5b^2$$

We know that $5|a^2$ and therefore $5|a$ (since if there is a 5 in the prime decomposition of a^2 there must also be a 5 in the prime decomposition of a).

So we can write $a = 5m$ and $25m^2 = 5b^2 \implies 5m^2 = b^2$ - and by repeating the same logic, we can show that $5|b$. But if 5 divides both a and b, then $\gcd(a, b) = 5k$ for some $k \in \mathbb{N}$, which is a contradiction with our initial assumption that $\gcd(a, b) = 1$ - so our original assumption, that $\sqrt{5}$ is rational, must be false. □

Q. 2 *How many positive integer divisors does 36 have?*

$36 = 2^2 \cdot 3^2$, so every factor of 36 will have the form $2^\alpha \cdot 3^\beta$ with $\alpha \in \{0, 1, 2\}$ and $\beta \in \{0, 1, 2\}$.

We can find all of the factors of 36 by combining the possible values of α and β in all possible combinations, so the total number of factors of 36 is $3 \times 3 = 9$, since we have 3 choices for α and 3 choices for β.

Q. 3 $n! = n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1$ *(called* n *factorial). How many trailing zeros are there in* $25!$*?*

Q. 4 *How many positive integer factors does 720 have?*

Q. 5 *Write all the factors of* 7^{21} *and compute their sum.*