Number Theory notes

November 18, 2020

1 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!

2 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.

2.1 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.*

3 Modular arithmetic

Let's start this section with a question: 3.141592653589793238462643383279 is the value of π to 30 decimal places. Is the number 3141592653589793238462643383279 the square of an integer?

Rather than attempting to answer ths question directly, let's do some exploration of squares of integers, to see if we can find some common characteristics.

n	n^2	$\text{rem}(\frac{n^2}{4})$
1	1	1
2	4	0
3	9	1
4	16	0
5	25	1
6	36	0
7	49	1

Interestingly, it seems like every even square has a remainder of 0 when we divide by 4, and every odd square has a remainder of 0. We can prove that this is the case in general quite easily:

$$n = 2k \implies n^2 = 4k^2$$
$$n = 2k+1 \implies n^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$$

We can now return to our original question - a simple initial test for whether a number is a square of an integer is to check its remainder when divided by 4. And we only need to look at the last two digits to check because $100n + m = 4(25n) + m$ - so we can ignore everything before the last 2 digits. In our example, $79 = 4 \times 19 + 3$, so the number at the start of this section is **not** the square of an integer.

3.1 Working with remainders

This example gives a glimpse of something called modular arithmetic - sometimes, we can draw conclusions related to a problem by looking only at the remainders when divided by a number. In terms of notation, we say that $a \equiv b \pmod{n}$ when $a = m \cdot n + b$ for some integer m. In the example above, we can write: $a^2 \equiv 0 \text{ or } 1 \pmod{4}$ for all $a \in \mathbb{Z}$.

There are a few operations that hold for all numbers $\pmod{n}$:

Remainders are additive and multiplicative:

$$\begin{aligned}(a \pmod n) + (b \pmod n) &= (a+b) \pmod n \\ (a \pmod n) \cdot (b \pmod n) &= (a \cdot b) \pmod n\end{aligned}$$

So we can tell that if $a = 76$ and $b = 42$, when we multiply them together, the remainder when we divide the result by 5 will be $76 \pmod 5) \times 42 \pmod 5) = 1 \times 2 \pmod 5)$. We say that $a \equiv b \pmod n$ (a is congruent to b mod n) if $n|(a-b)$ - that is, if we subtract one number from another, and they have the same remainder when divided by n, then their difference is a multiple of n.

Just the basics of modular arithmetic allow us to address a whole range of problems already.

Q. 6 *Prove that* $6 \cdot 4^n - 6$ *is divsible by 9 for all n.*

Proof: Let's look at the values of $6 \cdot 4^n \pmod 9$ for different values of n.

n	$4^n \pmod 9$	$6 \cdot 4^n \pmod n$
0	1	6
1	4	6
2	7	6
3	1	6

Clearly, 4^n cycles through the values 1, 4, 7 for all n, and each of these multiplied by 6 gives a remainder of 6 when divided by 9. Another way of putting this is that $4^n \equiv 1 + 3k \pmod 9$ for $n \equiv k \pmod 3$, and since $6 \cdot 3 = 18 \equiv 0 \pmod 9$ $6 \times (1 + 3k) \equiv 6 \pmod 9$ for all n.

Q. 7 *What are the last two digits base 10 of* 6^{19}*?*

Answer: This is an intimidating looking question, but modular arithmetic offers us a powerful tool to simplify things. $6^2 = 36 \pmod{100}$, $6^3 = 216 \equiv 16 \pmod{100}$, $6^4 \equiv 96 \pmod{100} \equiv -4 \pmod{100}$, $(6^4)^2 = 6^8 \equiv (-4^2) = 16 \pmod{100}$ So we have $6^8 \equiv 6^3 \pmod{100}$ But now we have:

$$\begin{aligned}6^{19} &= (6^8)^2 \cdot 6^3 \\ &\equiv (6^3)^3 \pmod{100} \\ &\equiv 6^9 \pmod{100} \\ &\equiv 6^8 \cdot 6 \pmod{100} \\ &\equiv 6^4 \pmod{100} \\ &\equiv 96 \pmod{100}\end{aligned}$$

You can use modular arithmetic to prove common divisibility tricks.

Q. 8 *Prove that 9 divides a number if and only if it divides the sum of its digits.*

Q. 9 *Prove that a number is divisible by 8 if its last 3 digits are divisible by 8.*

Q. 10 *Prove that a number is divisible by 11 if the sum of its even digits minus the sum of its odd digits is divisible by 11.*