MY NOTES ON NUMBER THEORY

Cornelius Schätz

Contents

1 Introduction to Numbers

1.1 Types of Numbers

Our relationship to the world of mathematics started when we began to count things. 30 people in our tribe, 20 trees around us, 2 dead cows to eat. We ordered the numbers so we knew that 30 people are more than 28 people - which was the actual amount of people in your tribe. Two new guys joined you this morning. We needed to add numbers up. We needed to multiply things. And it all went fine with the numbers we used for counting, the natural numbers or positive integers. But when it came to the operation of subtraction, we were facing a problem. Sometimes the result of this process was a number less than zero, so less than nothing. Negative numbers stepped into the game and here we are now with the integers. But that was not enough either. Because in our daily life we also had to divide numbers. But the results of this division operations sometimes were not integers. A new realm of numbers was unlocked: the rational numbers. The crazy thing about them was that they could get arbitrarily small. You could think of the smallest rational possible, but all you had to do to make it smaller is add 1 to the denominator. Notice that those wild number fields only were uncovered by our interest in quantifying the world around us. We began to get a glimpse at the underlying foundation of the universe around us: the logic of mathematics. When we humans started to develop an interest in geometry, we discovered that there are numbers, which cannot even be expressed as a fraction of integers. Non-rational numbers or as we call them now: irrational numbers. It has been a disciple of Pythagoras who seemed to have found out, that in a right triangle with the two right angle sides being of length 1 the hypotenuse has to be an irrational number ($\sqrt{2}$). Apparently he got thrown into the ocean for pointing this out. The ancient greek were especially interested in geometrically constructing everything, especially numbers. They asked themselves if it is possible to just use straightedge and compass and construct a square the size of a circle. This problem reduces to geometrically constructing a distance between to points of length π. It took almost two thousand years to prove that this is impossible. By showing that π cannot be expressed as the solution to an algebraic equation. And all numbers that can be constructed geometrically can also be expressed as solutions to algebraic equations. But it got even weirder. We have already known for quite some time that there is an infinity of numbers. But less than 200 years ago Georg Cantor found out that there are different types of infinity. Some sets of numbers are bigger than others - although all of those sets have an infinite amount of elements. So to begin building a foundation for understanding number theory we start by understanding the foundation of numbers themselves: infinity.

1.2 Infinity

1.2.1 Countability

1.2.2 Even and Odd Numbers

1.2.3 Integers and Naturals

1.2.4 Rationals and Naturals

1.2.5 Reals are more than infinite

2 Prime Numbers

2.1 What are Prime Numbers

When we talk about the natural numbers, we can either differentiate them into even and odd or prime and composite. Prime Numbers are numbers whose only divisors are 1 and themselves. The first examples are $2, 3, 5, 7, 11, ...$ Composite numbers are numbers, which are a product of prime numbers, for example $12 = 2 \cdot 2 \cdot 3$. As it will turn out in the next section, all numbers are either composite or prime. And not only that, all composite numbers have a unique prime factorization. This means that there is a specific sequence of primes for every number you can think of. The prime numbers therefore form somehow the atoms of the world of numbers. Let's jump right in and learn a bit more about primes.

2.2 Composites and Primes

Theorem 2.1. Every $n > 1, n \in \mathbb{N}$ can be expressed as a product of primes.

This is known as the prime factorization of a positive integer. The prime factorization of a prime number p would be $p = 1 \cdot p$. Let's prove this theorem.

Proof. We go by contradiction. First we assume that there are a bunch of numbers $\{n_i\}$ which do not have a prime factorization. Since the natural numbers are an ordered set of numbers, there must exist a smallest number n_0 without a prime factorization. If n_0 were prime, it would have a prime factorization. Therefore n_0 must be composite. That means there exist $a, b < n_0$ such that $n = a \cdot b$. But both a and b must have a prime factorization, since n_0 was the smallest number without one. So there exist prime numbers $p_1, ..., p_a$ and $q_1, ..., q_b$ such that:

$$a = p_1 \cdot ... \cdot p_a \tag{1}$$

$$b = q_1 \cdot ... \cdot q_b \tag{2}$$

And since $n_0 = a \cdot b$ we get:

$$n_0 = a \cdot b = p_1 \cdot ... \cdot p_a \cdot q_1 \cdot ... \cdot q_b \tag{3}$$

So n_0 does have a prime factorization! That is a contradiction to our initial assumption that n_0 is the smallest number without a prime factorization. Therefore such a number cannot exist. □

2.3 Divisibility by a prime

Theorem 2.2. If $p \mid ab$ then either $p \mid a$ or $p \mid b$.

Proof. We prove by contradiction. We start with $p \mid ab$ and assume that $p \nmid a$ and $p \nmid b$.

This means that

$$a = k_1 \cdot p + r_1 \tag{4}$$
$$b = k_2 \cdot p + r_2 \tag{5}$$

with $r_1, r_2 \neq 0$. Now we multiply them:

$$ab = (k_1 \cdot p + r_1)(k_2 \cdot p + r_2) = \tag{6}$$
$$k_1 k_2 p^2 + k_1 r_2 p + k_2 r_1 p + r_1 r_2 = \tag{7}$$
$$(k_1 k_2 p + k_1 r_2 + k_2 r_1) \cdot p + r_1 r_2 = \tag{8}$$
$$m \cdot p + r_1 r_2 \tag{9}$$

with $m = k_1 k_2 p + k_1 r_2 + k_2 r_1 \in \mathbb{Z}$ and $r_1 r_2 \neq 0$, which means that $p \nmid ab$, which is a contradiction to the initial condition. Therefore at least one of the two a, b must be dividable by p. □

2.4 The fundamental theorem of Arithmetic

We now know that every natural number is either a composite or a prime, it is now time to dive a bit deeper and learn about the fundamental theorem of Arithmetic. Not only does every positive integer have a prime factorization, but this factorization is also unique. This means that there is only one combination of primes for every natural number. The primes form the atoms of the natural number and each natural number is individual because it has a unique composition of primes. Let's write the theorem down and prove it.

Theorem 2.3. Every $n > 1, n \in \mathbb{N}$ has a unique prime factorization.

Proof. We show the correctness of this theorem in a similar way like we did for the last one. We start by assuming the contrary: there exists a set of numbers $\{n_i\}$ which have more than one prime factorization. And since the natural are ordered, there must exist a smallest element n_0 with more than one prime factorization. For simplicity we assume that n_0 has only two different factorizations. We are going to prove that that those two must be identical. So the two factorizations shall look like this:

$$n_0 = p_1 \cdot ... \cdot p_a n_0 = q_1 \cdot ... \cdot q_b \tag{10}$$

According to Theorem 2.2 there must exist a p that divides at least one of the prime numbers q. Without loss of generality we can assume that $p_1 \mid q_1$. But since q_1 is a prime, $p_1 \mid q_1$ means that $p_1 = q_1$. Therefore we get:

$$\frac{n_0}{p_1} = p_2 \cdot ... \cdot p_a = q_2 \cdot ... \cdot q_b = \frac{n_0}{q_1} \tag{11}$$

But both $p_2 \cdot ... \cdot p_a < n_0$ and $q_2 \cdot ... \cdot q_b < n_0$. And n_0 was the smallest number with more than one prime factorization, every smaller number does have a unique factorization. Since the two products are equal to each other and both result in a number smaller than n_0, the

primes must be the same:

$$a = b \quad \Rightarrow \quad p_2 = q_2 \ ... \ p_a = q_a \tag{12}$$

So n_0 does not have two prime factorization. Therefore there cannot exist a smallest number with more than one factorization, so all positive integers must have a unique prime factorization. □

2.5 The infinity of primes

Theorem 2.4. There is infinitely many primes.

Proof. The idea of this proof traces back over 2000 years to Euklid. Assume there is only a finite amount of prime numbers $p_1, ..., p_n$. Now we construct a new number Q:

$$Q = p_1 \cdot ... \cdot p_n + 1 \tag{13}$$

Since we have already proven that every positive integer has prime factors, there must exist at least one p amongst the finitely many primes $p_1, ..., p_n$ which divides Q:

$$\exists p \in \{p_1, ..., p_n\} : p \mid Q \tag{14}$$

But since $p \in \{p_1, ..., p_n\}$ we also get

$$p \mid p_1 \cdot ... \cdot p_n \tag{15}$$

From this we can conclude that

$$p \mid (Q - p_1 \cdot ... \cdot p_n) \ \Rightarrow \ p \mid 1 \tag{16}$$

But since $p > 1$ is a prime number, it cannot divide 1. Therefore we arrived at a contradiction. There cannot be only a finite number of primes. □

2.6 Every $n \geq 12$ is the sum of 2 composites

In the context of primes and composites we have only been interested in the operation of multiplication and prime factors. Another interesting way of constructing numbers is not by multiplying them but by adding them. As we will see, almost all numbers can be expressed as the sum of two composite numbers, and this is valid for prime numbers as well. Take the prime number 13 for example. 13 = 9 + 4. Both 9 and 4 are composite. One step further we got 14 = 10+4. This seems to work for all numbers. Most interestingly for all numbers greater or equal than 12. For smaller numbers it does not always work. It works for 10 for example (10=6+4, both terms are composite), but not for 11 (9+2, 8+3, 7+4, 6+5, at least one term is prime). So 12 seems to be some magical boundary. From here on every number can be expressed as the sum of two composites. And we shall prove this now.

Theorem 2.5. Every $n \geq 12$ is the sum of two composite numbers.

Proof. Any $n \geq 12$ can either be even or odd. Let's start by assuming n is even, so there exists a $k \in \mathbb{Z}, k > 2$ such that $n = 2k$. Now two find out how we can express this number as the sum of two composites we can start by subtracting a composite number and adding it again. The first possible composite number would be 4. So we get:

$$n = n - 4 + 4 = 2k - 4 + 4 = (2k - 4) + 4 \tag{17}$$

One of the two terms in the sum is a composite (the number 4). We have to show that $2k - 4$ is composite. We just rewrite it as:

$$2k - 4 = 2(k - 2) \tag{18}$$

So it is also composite. Therefore any even n bigger than 12 can be expressed as the sum of two composites. All there is left are the odd numbers. So let's assume n is odd. So there exists a $k \in \mathbb{Z}, k > 2$ such that $n = 2k + 1$. Now we apply the same strategy as before by subtracting a composite number and adding it again. But the number 4 in this case does not work. We would get $n - 4 + 4 = 2k + 1 - 4 + 4 = (2k - 3) + 4$ and we cannot tell anything about $2k - 3$, it could be composite or prime. The same problem appears for the next composite number 6. And for 8 as well. This is because we are dealing with odd numbers, so we should choose an odd composite to subtract and add again. And the first possible composite odd number is 9. So in the case of n being odd we get:

$$n = n - 9 + 9 = 2k + 1 - 9 + 9 = (2k - 8) + 9 \tag{19}$$

The first term is even and therefore composite, the second term is 9 and composite. So odd numbers as well can be expressed as the sum of two composites!

□

2.7 $n^4 + 4$ can never be prime

This is a wonderful simple theorem which we can easily prove by applying some binomial formulas. I find it wonderful because it is so hard to find a pattern to the prime numbers but still they sometimes reveal some secrets to us. And this secret tells us that no number of the form $n^4 + 4$ for $n > 1$ can ever be prime. Let's have a look at the proof.

Theorem 2.6. For every $n > 1$ the number $n^4 + 4$ is composite.

Proof. Never being prime or always composite - two sides of the same coin. We will show that $n^4 + 4$ must be composite. Let's rewrite it a little:

$$n^4 + 4 = (n^2)^2 + 2^2 = (n^2)^2 + 2^2 + 2 \cdot 2 \cdot n^2 - 2 \cdot 2 \cdot n^2 \tag{20}$$

Here we have just added 0. This we can rewrite as a binomial formula:

$$(n^2)^2 + 2^2 + 2 \cdot 2 \cdot n^2 - 2 \cdot 2 \cdot n^2 = (n^2 + 2)^2 - (2n)^2 \tag{21}$$

Now comes the last binomial formula:

$$(n^2 + 2)^2 - (2n)^2 = (n^2 + 2 - 2n)(n^2 + 2 + 2n) \tag{22}$$

And this is it. We have shown that $n^4 + 4$ can always be expressed as the product of two natural numbers bigger than 1. So it can never be prime.

□

2.8 Mersenne numbers

In the early 1600's Marin Mersenne was studying prime numbers of the form $2^n - 1$. It seemed like plugging in primes for n resulted in a prime. But it only seemed like it. If you plug in $n = 11$, you get 2047 as a result, which is a composite number. So here we can not just draw a conclusion. All of the numbers of the form $2^n - 1$ which are prime are called Mersenne numbers. And related to them is an interesting little theorem. If $2^n - 1$ is a prime number than we can conclude that n must be prime as well. Or phrasing it differently: If n is composite then $2^n - 1$ must be as well.

Theorem 2.7. If $2^n - 1$ is a prime number than n is a prime number as well.

Proof. We show this by assuming that n is composite and concluding that $2^n - 1$ must be composite as well for any n. Let's take a step sidewards and look at the finite geometric sum:

$$S = 1 + x + x^2 + ... + x^{n-1} \tag{23}$$

There is a simple formula for a sum of this type and we can easily derive it. First multiply the sum by x.

$$xS = x + x^2 + ... + x^n \tag{24}$$

Now we subtract this from the original sum:

$$S - xS = S(1 - x) = 1 - x^n \tag{25}$$

So we get that the sum S can be written as:

$$S = \frac{1 - x^n}{1 - x} = \frac{x^n - 1}{x - 1} \tag{26}$$

On the other hand we can write $x^n - 1$ as:

$$x^n - 1 = (x - 1)(1 + x + ... + x^{n-1}) \tag{27}$$

Now let's return to our orginal problem with the Mersenne primes. For n being composite we can write $2^n - 1$ as:

$$2^n - 1 = 2^{pq} - 1 = (2^p)^q - 1 \tag{28}$$

Comparing this with 27 we can identify

$$x = 2^p \tag{29}$$

So eventually:

$$2^n - 1 = 2^{pq} - 1 = (2^p)^q - 1 = (2^p - 1)(2^{p(q-1)} + ... + 1) \tag{30}$$

So $2^n - 1$ can be written as the product of two numbers that are bigger than one. Therefore it is composite. So n composite lead to $2^n - 1$ being composite. This in return means that $2^n - 1$ being prime will only work with n being prime. Nonetheless some prime numbers like 11 create a composite number.

□

Some interesting fact about the Mersenne numbers is that we do not know how many of them there are. It could be infinitely many or just a finite amount.

2.9 Fermat Numbers

After investigating Mersenne numbers it is time to investigate Fermat numbers, which are numbers that are of the form 2^n+1 with n being a power of 2. Fermat thought that numbers of the form $2^{2^n} + 1$ would always be prime for any positive integer n. The first five Fermat numbers are indeed prime:

$$F_0 = 3 \quad F_1 = 5 \quad F_2 = 17 \quad F_3 = 257 \quad F_4 = 65,537 \tag{31}$$

But in 1732 Euler found out that $F_5 = 2^{32} + 1$ is composite which disproved Fermat's idea. Nonetheless there exists a relationship between $2^n + 1$ being prime and n being the power of 2. This brings us to this interesting little theorem.

Theorem 2.8. If $2^n + 1$ is prime then n is a power of 2.

Proof. Similarily to the last section, in which we were dealing with Mersenne numbers, we will approach the proof of this theorem from the other side. Just because n is a power of 2 does not mean that $2^n + 1$ is prime, but whenever it is then n must be a power of 2. This on the other hand means that the case of n not being a power of 2 would always result in a composite number. So let's assume that n is not a power of 2. This means we have some power of 2 multiplied by some odd number d:

$$n = d \cdot 2^k \tag{32}$$

So we want to show that

$$2^n + 1 = 2^{d \cdot 2^k} + 1 = (2^{2^k})^d \ + \ 1 \tag{33}$$

is a composite number.

Now we are going to take a look at the geometric sum again but this time for negative x values:

$$1 - x + x^2 \pm ... + x^{n-1} = \frac{x^n + 1}{x + 1} \tag{34}$$

for $n - 1$ being even or n being odd. So we get:

$$x^n + 1 = (x + 1)(x^{n-1} \pm ... + 1) \tag{35}$$

This we can now apply to our original problem by identifying

$$x = 2^{2^k} \tag{36}$$

So we eventually get

$$2^n + 1 = 2^{d \cdot 2^k} + 1 = (2^{2^k})^d + 1 = \tag{37}$$

$$(2^{2^k} + 1)(2^{2^k(d-1)} \pm ... - 2^{2^k} + 1) \tag{38}$$

Now we only have to show that the long term in the second bracket is bigger than one.

$$(2^{2^k(d-1)} \pm ... - 2^{2^k} + 1) = ((2^{2^k(d-1)} - 2^{2^k(d-2)} \pm ...2^{2 \cdot 2^k} - 2^{2^k} + 1) > 0 + ...0 + 1 = 1 \tag{39}$$

So it indeed is always bigger than 1 and we can conclude that an input which is not a power of 2 will not yield a prime - never. So we also have proven that whenever $2^n + 1$ is prime n has to be a power of 2. □

Similar to the Mersenne numbers we have zero idea how many Fermat numbers there are. It could be infinitely many but also only finitely many.

2.10 Perfect nummbers

Another interesting part of number theory is that of perfect numbers, which is closely related to the Mersenne primes. Perfect numbers have already been investigated by Euklid over 2000 years ago. So what is a perfect number? Must be something really rare, since its perfect. They are indeed very rare. And we know little about them. Here a definition:

Definition 2.1. A perfect number is the sum of its divisors excluding itself.

That's quite an easy definition, isn't it? The first perfect number is 6:

$$6 = 1 + 2 + 3 \tag{40}$$

The next one is 28:

$$28 = 1 + 2 + 4 + 7 + 14 \tag{41}$$

When Euklid was working on them, he found out (and could prove) that every number of the form

$$2^{p-1}(2^p - 1) \tag{42}$$

is perfect if both p and $2^p - 1$ are prime. Or in other words: If $2^p - 1$ is a Mersenne prime, then $2^{p-1}(2^p - 1)$ is a perfect number. Some eternity later Euler put one on top. He could show that if an even number n is perfect, then it must be of the type $2^{p-1}(2^p - 1)$ with $2^p - 1$

being prime. Notice the little addition "even". We do not know anything about uneven perfect numbers. In fact we do not even know if they exist. But at least we can gain some knowledge about the even ones. But how can we prove both Euklid's and Euler's theorem? We will have to introduce the so called divisor function.

2.10.1 The divisor function

Without talking too much we jump right into the definition of the divisor function.

Definition 2.2. The divisor function $\sigma(n)$ of a positive integer n is the sum of all divisors of n including n itself.

$$\sigma(n) = \sum_{d|n} d \tag{43}$$

So let's just straight apply that definition to some examples, starting with the perfect number 6:

$$\sigma(6) = 1 + 2 + 3 + 6 = 12 \tag{44}$$

We see that the divisor function here equals double the original number. Let's have a look at a prime number:

$$7 = 1 + 7 = 8 \tag{45}$$

Nothing special about that. The only numbers dividing a prime number are 1 and the number itself. The divisor function has an interesting and for us useful property which is being multiplicative.

Theorem 2.9. Let $n = pq$ and $(p, q) = 1$ then $\sigma(pq) = \sigma(p) \cdot \sigma(q)$.

Proof.

$$\sigma(n) = \sigma(pq) = \sum_{d|pq} d = \sum_{r|p\ ,\ s|q} rs \tag{46}$$

Where r are the divisors of q and s are the divisors of q. Since the greatest common divisor of p and q is one, none of the r and s are the same. The product rs then gives a number which divides the product pq. This one sum can be changed into a product of two sums referring to r and s separately which finally proves the theorem:

$$\sum_{r|p\ ,\ s|q} rs = \Big(\sum_{r|p} r\Big) \cdot \Big(\sum_{s|q} s\Big) = \sigma(p) \cdot \sigma(q) \tag{47}$$

Now how is the divisor function related to Euclid's perfect numbers? The first thing we notice is that Euclid's definition does not include the number itself in the sum, unlike the divisor function. So the definition of a perfect number in terms of the divisor function is:

Definition 2.3. A perfect number n satisfies the equation

$$\sigma(n) = 2n \tag{48}$$

Now before we can go on to Euclid's way of constructing perfect numbers we have to look at the divisor function with prime powers as an argument. Let p be a prime and a

some integer power. The divisor function of p^a is:

$$\sigma(p^a) = 1 + p + p^2 + ... + p^a \tag{49}$$

This is a geometric sum and can be expressed with the simple fraction:

$$\sigma(p^a) = \frac{p^{a+1} - 1}{p - 1} \tag{50}$$

Now we are fully equipped to construct perfect numbers.

2.10.2 Euclid's Perfect Number Theorem

Theorem 2.10. If $2^p - 1$ is prime (with p being prime as well) then

$$n = 2^{p-1}(2^p - 1) \tag{51}$$

is a perfect number.

Proof. Since $(2^p - 1)$ is an odd prime and 2^{p-1} a power of 2, $(2^{p-1}, (2^p - 1)) = 1$ and therefore we can appyl the multiplicativity of the divisor function:

$$\sigma(2^{p-1}(2^p - 1)) = \sigma(2^{p-1}) \cdot \sigma(2^p - 1) \tag{52}$$

Now for the first factor we have a power of prime number as an argument and therefore we can apply the geometric sum:

$$\sigma(2^{p-1}) = \frac{2^p - 1}{2 - 1} = 2^p - 1 \tag{53}$$

Now for the second factor we know that the argument is prime so the only divisors are 1 and itself:

$$\sigma(2^p - 1) = 1 + (2^p - 1) = 2^p \tag{54}$$

We can finally conclude:

$$\sigma(2^{p-1}(2^p - 1)) = \sigma(2^{p-1}) \cdot \sigma(2^p - 1) = (2^p - 1) \cdot 2^p = 2 \cdot 2^{p-1}(2^p - 1) = 2n \tag{55}$$

□

2.10.3 The Euler-Euclid-Theorem

With Euclid's theorem about perfect numbers we have a way to construct perfect numbers. But that does not tell us if all perfect numbers have that form that Euclid used. Euler could prove that indeed all even perfect numbers are of the Euclid type. This is nowadays known as the Euler-Euclid Theorem and we are going to prove it.

Theorem 2.11. If a positive integer n is even and perfect then

$$\exists\, p \in \mathbb{N} \;:\; n = 2^{p-1}(2^p - 1) \tag{56}$$

Proof. Since n is an even number we can express it as some power of two times some odd number d:

$$n = 2^{p-1} \cdot d \tag{57}$$

I have chosen $p-1$ as an exponent so it later fits perfectly the form above. This is something one does not know upfront when constructing the proof. Now we also know that n is a perfect number, so:

$$\sigma(n) = 2n \tag{58}$$

Or by plugging in 58:

$$\sigma(n) = \sigma(2^{p-1}d) = \sigma(2^{p-1}) \cdot \sigma(d) \tag{59}$$

Here we could apply the multiplicativity of the divisor function because the greatest common divisor of 2^{p-1} and d is 1. Now

$$\sigma(2^{p-1}) = 2^p - 1 \tag{60}$$

So we get:

$$\sigma(n) = \sigma(2^{p-1}) \cdot \sigma(d) = (2^p - 1) \cdot \sigma(d) \overset{!}{=} 2 \cdot 2^{p-1} \cdot d = 2^p d \tag{61}$$

Or to have it more clear:

$$(2^p - 1) \cdot \sigma(d) \overset{!}{=} 2^p \cdot d \tag{62}$$

Now $(2^p - 1) \mid 2^p d$ but $((2^p - 1), 2^p) = 1$ so $(2^p - 1) \mid d$ which means there has to exist some integer m such that

$$d = (2^p - 1)m \tag{63}$$

Plugging that into 62 we get:

$$(2^p - 1) \cdot \sigma(d) \overset{!}{=} 2^p \cdot (2^p - 1) \cdot m \tag{64}$$

Which leads us to concluding that

$$\sigma(d) = 2^p \cdot m \tag{65}$$

Now on the other hand we know that m and d are divisors of d so the divisor function has to be at least the sum of those two divisors:

$$\sigma(d) \geq m + d = m + (2^p - 1) \cdot m = m + 2^p \cdot m - m = 2^p \cdot m \tag{66}$$

This can only mean that m and d are the only divisors of d and therefore d has to be prime and $m = 1$. So finally we get

$$d = 2^p - 1 \tag{67}$$

And since $n = 2^{p-1} \cdot d$ we get

$$n = 2^{p-1}(2^p - 1) \tag{68}$$

□

2.11 Fermat's little theorem

Let's take some random integer number like 6 and choose a prime number like 2. Now if we divide 6 by 2 we get a remainder of zero. If raise 6 to the power of 2 we get 36, which again gives zero when dividing by 2. What we just observed is true for all integers raised to the power of a prime. And this is known as Fermat's little theorem.

Theorem 2.12. Let $a \in \mathbb{Z}$ and p be a prime number. Then

$$a^p = a \, mod \, p \tag{69}$$

meaning that a^p has the same remainder when dividing by p as a itself has. The theorem is sometimes also written as

$$a^{p-1} = 1 \, mod \, p \tag{70}$$

Proof. We will prove this via induction. The first step of induction would be to take the number 2 for example, raise it to the power of 2 and see that both 4 and 2 have the same remainder when dividign by 2. So let's go to the real tricky part.
Let's say the theorem is true for a, so $a^p = a \, mod \, p$. We now want to show that under this condition it must also be true for $a + 1$ meaning that $(a + 1)^p = (a + 1) \, mod \, p$. To show that we have to apply the binomial theorem.

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^p = a^p + \binom{p}{1} + ... \binom{p}{p-1} a + 1 \tag{71}$$

Now all the terms that include the binomial coefficient contain the prime p in the numerator and therefore give zero when dividing by p.

$$\left[\binom{p}{1} + ... \binom{p}{p-1} a \right] \; mod \, p = 0 \, mod \, p \tag{72}$$

So let's have a look at $a^p + 1$. From our first induction step we know that $a^p = a \, mod \, p$ so we can conclude:

$$(a^p + 1) \, mod \, p = (a + 1) \, mod \, p \tag{73}$$

which is exactly what we anticipated to show. Wonderful!

□

2.12 Arithmetical progressions of the type $4n - 1$ and $4n + 1$

We can now use our knowledge of Fermat's little theorem and apply it to the understanding of some special arithmetic progressions. One easy arithmetic progression we already know is the progression of odd numbers $2n + 1$. And we also know that this progression contains infinitely many primes. This makes you wonder what other arithmetical progressions there might be which contain an infinite amount of prime numbers. Two such progressions are

the ones mentioned in the title of this section. We will show that both $4n-1$ and $4n+1$ contain an infinite amount of prime numbers and for the latter we will be applying Fermat's little theorem. The first one is easier to prove though so let's start with that.

Theorem 2.13. The arithmetical progression $4n-1$ contains infinitely many primes.

Proof. We will prove this via good old contradiction. We assume there is a finite amount of primes of the type $4n-1$. Let p be the biggest such prime. Now we construct a new number

$$N = 2 \cdot 2 \cdot 3 \cdot ... \cdot p - 1 \tag{74}$$

None of the prime numbers up to p divides N, so none of the prime factors of N can be of the form $4n-1$. But N itself is of the form $4n-1$ so it must have at least one prime factor of the form $4n-1$. Since all prime factors of N are bigger than the biggest prime number p of the form $4n-1$, this is a contradiction. So p is not the biggest such prime number and therefore there must exist infinitely many primes in this arithmetical progression. □

Theorem 2.14. The arithmetical progression $4n+1$ contains infinitely many primes.

Proof. This is where we will finally apply Fermat's little theorem. In order to show that the progression $4n+1$ does indeed contain infinitely many primes we prove that for any positive integer N there exists a prime number p such that $p = 1 \, mod \, 4$. We start by defining a large number of the form $4n+1$ with this N:

$$m = (N!)^2 + 1 \; = \; 2^2 \cdot 3^2 \cdot ... \cdot N^2 + 1 \; = \; 4n + 1 \tag{75}$$

with $n = 3^2 \cdot ...N^2$. Now none of the prime factors q of N divides m, so the prime factors p of m must be bigger than N. So we can write for some p:

$$(N!)^2 + 1 \; = \; 0 \, mod \, p \tag{76}$$

This we can rewrite:

$$(N!)^2 = -1 \, mod \, p \tag{77}$$

Now we raise both sides of the equation to the power of $\frac{p-1}{2}$:

$$(N!)^{p-1} = (-1)^{\frac{p-1}{2}} \, mod \, p \tag{78}$$

Now from Fermat's little theorem we know that

$$(N!)^{p-1} = 1 \, mod \, p \tag{79}$$

So we can conclude:

$$(-1)^{\frac{p-1}{2}} \, mod \, p = 1 \, mod \, p \tag{80}$$

This gives us some important information about the exponent: it has to be even. So there exists a $k \in \mathbb{N}$ such that:

$$\frac{p-1}{2} = 2k \tag{81}$$

So we get for p:

$$p = 4k + 1 \tag{82}$$

This is it! A wonderful proof making use of Fermat's little theorem., □

3 Irrational Numbers

3.1 $\sqrt{2}$ is irrational - Pythagoras Proof

Proving that $\sqrt{2} \notin \mathbb{Q}$ is one of the basic exercises of number theory. In this section we will show this with the classical argument of even numbers. In the next section we will use our knowledge about prime numbers to prove the irrationality of $\sqrt{2}$. So as it is usual for irrationality proofs, we will start by assuming the contrary.
So let's assume that $\sqrt{2} \in \mathbb{Q}$ with $\sqrt{2} = \frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $gcd(a, b) = 1$. Let's have a closer look at the equation

$$\sqrt{2} = \frac{a}{b} \tag{83}$$

and square both sides of the equation. This will give us:

$$2 = \frac{a^2}{b^2} \;\Rightarrow\; 2\,b^2 = a^2 \tag{84}$$

This means that a^2 is an even number, because it can be expressed as 2 times some number - which in our case is b^2. The fact that a^2 is even means that a also is even. This is easy to see. There are only even and odd numbers. Let's say we have an even number n which can be expressed as 2 times some number integer k. Squaring n also gives us an even number.

$$n = 2k \;\Rightarrow\; n^2 = 4k^2 \;=\; 2 \cdot 2 \cdot k^2 \tag{85}$$

Now let's think of n as an odd number and then square it:

$$n = 2k + 1 \;\Rightarrow\; n^2 = 4k^2 + 4k + 1 = 2\,(2k^2 + 2k) \;+\; 1 \tag{86}$$

Here we see that an odd number squared always yields some even number plus one - which in the end is an odd number again. So applying this knowledge to our proof, we see that a^2 being even means that a has to be even too.
And since a is even, it can be expressed as the product of 2 times some integer c.

$$a = 2c \tag{87}$$

Now let's plug this new expression for a into 84. This will give us:

$$a^2 = 4c^2 = 2b^2 \;\Rightarrow\; b^2 = 2c^2 \tag{88}$$

Here we end up with a very peculiar result. Because the fact that a is even has led us to the result that b^2 is even, which means that b is even. But this is a contradiction to our assumption in the beginning: $\sqrt{2} = \frac{a}{b}$ with $gcd(a, b) = 1$. The greatest common divisor of both a and b is 1. But since both of those numbers are even, their greatest common divisor has to be at least 2. Therefore $\sqrt{2}$ cannot be expressed as a fraction.

3.2 $\sqrt{2}$ is irrational - Prime Number Proof

There is an even more elegant way to show that $\sqrt{2}$ is not a rational number and it makes use of our knowledge about prime numbers. To be more specific, we will need our knowledge about prime factorization. Every natural number can be expressed as a product of prime numbers and this product is unique. That means that for a number $n \in \mathbb{N}$ there is only one unique combination of primes. This will come very handy in a couple of moments.
So let's begin the way we began in the section before: Assuming that $\sqrt{2} \in \mathbb{Q}$ with $\sqrt{2} = \frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $gcd(a, b) = 1$. We can write again:

$$2 = \frac{a^2}{b^2} \;\Rightarrow\; 2b^2 = a^2 \tag{89}$$

Now the integer b has a unique prime factorization:

$$b = p_1 \cdot ... \cdot p_n \tag{90}$$

This means that every prime number p amongst the set of prime numbers $\{p_1, ..., p_n\}$ divides a^2:

$$\forall\, p \in \{p_1, ..., p_n\} :\;\; p \mid a^2 \tag{91}$$

From the section about the divisibility of natural number by prime numbers we know that:

$$p \mid (a \cdot b) \;\Rightarrow\; p \mid a \;\vee\; p \mid b \tag{92}$$

So the fact that p divides a^2 means it either divides a or a, which just means:

$$p \mid a^2 \;\;\Rightarrow\; p \mid a \tag{93}$$

So the prime factors p of b also divide the integer a, but initially we said that the greatest common divisor of both should be one: $gcd(a, b) = 1$. Therefore all prime numbers p have to be 1, which means that $b = 1$. But this cannot be the case, so we have a contradiction!

3.3 $\sqrt[n]{K^m}$ is either integer or irrational

Applying what we learned in the last section we can actually show quite easily that the n-th root of some integer will always be either an integer or irrational. The best example for an integer as a result is $\sqrt[3]{27} = 3$. Now how do we prove that any n-th root of an integer is either irrational or integer? We - once again - start by assuming the contrary.
Assume $\sqrt[n]{K^m} \in \mathbb{Q}$ with $\sqrt[n]{K^m} = \frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $gcd(a, b) = 1$. Now we raise the power on both sides of the equation:

$$\sqrt[n]{K^m} = \frac{a}{b} \;\Rightarrow\; K^m = \frac{a^n}{b^n} \;\Rightarrow\; K^m \cdot b^m = a^n \tag{94}$$

Now let's take a look once again at the integer b. We know that b has a unique prime factorization:

$$b = p_1 \cdot ... \cdot p_n \tag{95}$$

This means that every prime number p amongst the set of prime numbers $\{p_1, ..., p_n\}$ divides a^n:

$$\forall\, p \in \{p_1, ..., p_n\} :\ p \mid a^n \tag{96}$$

And just like we did it in the last section, we can now conclude that p also divides a. But once again we remember that the greatest common divisor of both a and b was supposed to be 1. Therefore the fact that p divides both a and b means that $p = 1$. But p just stands for any prime number in the set $\{p_1, ..., p_n\}$, so all of them have to be equal to 1. Which leads to $b = 1$. So either $\sqrt[n]{K^m}$ is an integer or irrational and cannot be expressed as a fraction of integers at all.

3.4 e is irrational

To prove that e is indeed an irrational number, we will follow the classical path of assuming the contrary. We assume that e can actually be expressed as a fraction of integers: $e \in \mathbb{Q}$ and $e = \frac{a}{b}$ with $a, b \in \mathbb{Z}$ and $gcd(a, b) = 1$. Now we remember that the Euler number is defined via the infinite series:

$$e = \sum_{n=0}^{\infty} \frac{1}{n!} = \frac{1}{1} + \frac{1}{2} + \frac{1}{2 \cdot 3} + ... \tag{97}$$

Now to prove that e cannot be expressed as a fraction of integers we will construct a number α dependent on e and show that a rational Euler Number would lead to α being an integer and smaller than one. This is a contradiction, since integers cannot be smaller than one. Let's start by constructing this number:

$$\alpha = k! \left(e - 1 - \frac{1}{2} - \frac{1}{2 \cdot 3} - ... - \frac{1}{k!}\right) \tag{98}$$

The number k shall be an integer bigger than b (the denominator of e). We will see in a moment why we have to choose k exactly like this. Now the contradiction part starts. First we plug in the fraction $\frac{a}{b}$ for e:

$$\alpha = k! \left(\frac{a}{b} - 1 - \frac{1}{2} - \frac{1}{2 \cdot 3} - ... - \frac{1}{k!}\right) = \tag{99}$$

$$= \frac{a \cdot k!}{b} - k! - \frac{k!}{2!} - \frac{k!}{3!} - ... - \frac{k!}{k!} = \tag{100}$$

$$\left(\frac{a \cdot k!}{b} - k! - \frac{k!}{2!} - \frac{k!}{3!} - ... - 1\right) \in \mathbb{Z} \tag{101}$$

All of the terms in the above equation are integers. Here we can finally see, why we have chosen k to be an integer bigger than b. Now we can be sure that $\frac{a \cdot k!}{b}$ is an integer, because

b is a part of the product $1 \cdot 2 \cdot ... \cdot k$. This was the first part of our proof. We have shown that our constructed and made up number α is an integer under the assumption that e is a rational number.
Now we plug in the original series definition of the Euler Number $e = \sum_{n=0}^{\infty} \frac{1}{n!}$ into our constructed number α:

$$\alpha = k! \left(e - 1 - \frac{1}{2} - \frac{1}{2 \cdot 3} - ... - \frac{1}{k!} \right) = \tag{102}$$

$$= k! \left(\sum_{n=0}^{\infty} \frac{1}{n!} - 1 - \frac{1}{2} - \frac{1}{2 \cdot 3} - ... - \frac{1}{k!} \right) = \tag{103}$$

$$k! \left(1 + \frac{1}{2} + \frac{1}{2 \cdot 3} + ... + \frac{1}{k!} + ... - 1 - \frac{1}{2} - \frac{1}{2 \cdot 3} - ... - \frac{1}{k!} \right) = \tag{104}$$

$$k! \left(\frac{1}{(k+1)!} + \frac{1}{(k+2)!} + \frac{1}{(k+3)!} ... \right) = \tag{105}$$

$$= \frac{1}{k+1} + \frac{1}{(k+1)(k+2)} + \frac{1}{(k+1)(k+2)(k+3)} + ... \tag{106}$$

Now we need to find a way to show that this last part of the above equation is smaller than one and therefore not an integer. We notice that the denominators in that infinite sum are increasing in size, so we can estimate:

$$\alpha = \frac{1}{k+1} + \frac{1}{(k+1)(k+2)} + \frac{1}{(k+1)(k+2)(k+3)} + ... < \tag{107}$$

$$< \frac{1}{k+1} + \frac{1}{(k+1)^2} + \frac{1}{(k+1)^3} + ... \tag{108}$$

This last sum looks a lot like a geometric series. Remember that a geometric series with its value is defined in the following way:

$$\sum_{n=0}^{\infty} x^n = \frac{1}{1-x} \quad for \mid x \mid < 1 \tag{109}$$

Applying this to the sum above we get:

$$\alpha = \frac{1}{k+1} + \frac{1}{(k+1)^2} + \frac{1}{(k+1)^3} + ... = \tag{110}$$

$$\sum_{n=1}^{\infty} \frac{1}{(k+1)^n} = \sum_{n=0}^{\infty} \frac{1}{(k+1)^n} - 1 = \tag{111}$$

$$\frac{1}{1 - \frac{1}{k+1}} - 1 = \frac{k+1}{k} - 1 = \frac{1}{k} < 1 \tag{112}$$

This is it. This is the contradiction we were looking for. First we used the assumption that e is a rational number to show that our constructed number α is an integer. Then we have used the actual definition of the Euler number via its Taylor series to show that α must be smaller than one. Therefore the assumption that e is a rational number does not cooperate with the actual definition of the Euler number. So e cannot be rational. Quod erat demonstrandum. Wondeful!

3.5 π is irrational

This proof is from Ivan Niven, which is a simplification of Hermite's proof.

Proof. As always we start by assuming the contrary, that π is rational, $\pi = \frac{a}{b}$, with $a, b \in \mathbb{Z}$. We now define the function:

$$f(x) := \frac{x^n(a - bx)^n}{n!} \tag{113}$$

Where n is arbitrary and about to become important later in the proof. Now we are using this function to define another function:

$$F(x) := f(x) - f''(x) + f^{(4)} + ... + (-1)^n f^{(n)}(x) \tag{114}$$

The proof consists of 3 parts:

- We prove that both $F(0)$ and $F(\pi)$ are integer.
- We prove that the integral $\int_0^\pi f(x)sin(x)dx = F(0) + F(\pi) \in \mathbb{Z}$
- We show that the integral will be smaller than 1 for arbitrarily large n. This will create our desired contradiction.

1. $F(0)$ and $F(\pi)$ are integer

We begin with $F(0)$ and therefore we have to take a look at $f(0)$ and its derivatives. First of all, from 113 we can conclude that $f(0) = 0$. To investigate the derivatives we will use the binomial theorem to expand $f(x)$:

$$f(x) = \frac{1}{n!} \sum_{k=n}^{2n} c_k x^k \tag{115}$$

with c_k being integer coefficients, which is a mixture of a, b and the binomial coefficients. We are only interested in showing that $F(0)$ and $F(\pi)$ are integer, so the exact value of the coefficientes is of no importance. The sum begins with $k = n$ because n is the smallest exponent in the resulting polynomial whereas the highest exponent will be $2n$. Now we got everything to investigate the derivatives.

$$f^{(k)}(0) = \frac{c_k}{n!} k! \tag{116}$$

because the k-th derivative of the x^n-term (with k-starting at n) is 1. Therefore we remain with constant factor. All the other derivatives vanish when we plug in zero. The value for the k-th derivative is an integer (because $k! \geq n!$. So now we now that all derivatives evaluated at zero are integer. Therefore $F(0) \in \mathbb{Z}$ must hold as well. Now we have to do the same thing with $F(\pi)$. We start by taking a look at $f(\pi - x)$:

$$f(\pi - x) = \frac{(\pi - x)^n(a - b(\pi - x))^n}{n!} \tag{117}$$

Let's rewrite this a little bit:

$$f(\pi - x) = \frac{(\pi - x)^n (a - b\pi + bx)^n}{n!} =$$

$$\frac{(\frac{a}{b} - x)^n (a - a + bx)^n}{n!} = \frac{b^n x^n (\frac{a}{b} - x)^n}{n!} =$$

$$= \frac{x^n (a - bx)^n}{n!} = f(x)$$

Now we take a look at the derivatives using the chain rule:

$$f^{(k)}(\pi - x) = (-1)^k f^{(k)}(x) \tag{118}$$

So from this we can conclude

$$f^{(k)}(\pi) = (-1)^k f^{(k)}(0) \tag{119}$$

and therefore also $F(\pi)$ has to be an integer. We have finished the first part of our proof showing that both

$$F(0),\, F(\pi) \,\in\, \mathbb{Z} \tag{120}$$

2. Show that $\int_0^\pi f(x)sin(x)dx = F(0) + F(\pi) \in \mathbb{Z}$

Now we will prove that the integral $\int_0^\pi f(x)sin(x)dx$ is integer under the condition that $\pi \in \mathbb{Q}$. We start by looking at the second derivative of $F(x)$:

$$F''(x) = f''(x) - f^{(4)} + ... + f^{(2n)}(x) \tag{121}$$

Since $f(x)$ is maximally of degree $degf = 2n$ we can conclude that $f^{(2n)}(x) = 0$. This leads us to

$$F''(x) + F(x) = f(x) \tag{122}$$

Multiplying both sides of the equation with $sin(x)$ gives us:

$$F''(x)sin(x) + F(x)sin(x) = f(x)sin(x) \tag{123}$$

Applying the product rule for derivatives backwards we get

$$(F'sin)' = F''sin + F'cos \;\Rightarrow\; F''sin = (F'sin)' - F'cos$$
$$(-Fcos)' = Fsin - F'cos \;\Rightarrow\; Fsin = F'cos - (Fcos)'$$

So for $f(x)sin(x)$ we now get:

$$f(x)sin(x) = (F'(x)sin(x))' - F'(x)cos(x) + F'(x)cos(x) - (F(x)cos(x))' =$$
$$(F'(x)sin(x))' - (F(x)cos(x))' = (F'(x)sin(x) - F(x)cos(x))'$$

Now we can finally evaluate the integral:

$$\int_0^\pi f(x)sin(x)dx =$$

$$= F'(\pi)sin(\pi) - F(\pi)cos(\pi) - F'(0)sin(0) + F(0)cos(0) =$$

$$= F(\pi) + F(0) \in \mathbb{Z}$$

We are finally ready to go to the final step and create our contradiction.

3. Show that $\int_0^\pi f(x)sin(x)dx < 1$

Let's explicitly write down the integral:

$$\int_0^\pi f(x)sin(x)dx = \int_0^\pi \frac{x^n(a-bx)^n}{n!}sin(x)dx \tag{124}$$

Now we take a look at the numerator of the fraction. Since $0 < x < \pi$ we can estimate:

$$x^n(a-bx)^n \leq \pi^n(a-bx)^n \leq (\pi a)^n \tag{125}$$

Additionally we know that $0 \leq sin(x) \leq 1$ for all x smaller than π. So for the integral we can conclude:

$$\int_0^\pi \frac{x^n(a-bx)^n}{n!}sin(x)dx \ \leq \ \int_0^\pi \frac{(\pi a)^n}{n!} \cdot 1dx = \frac{(\pi a)^n}{n!}\int_0^\pi dx = \frac{(\pi a)^n}{n!} \cdot \pi \tag{126}$$

This last expression gets arbitrarily small since n is a parameter that can be chosen arbitrarily big. Therefore we see that

$$\int_0^\pi \frac{x^n(a-bx)^n}{n!}sin(x)dx \ < \ 1 \tag{127}$$

But in the previous step we have shown that the integral takes an integer value, which is a contradiction to the conclusion of the third step. There does not exist an integer smaller than 1. Therefore our initial assumption of π being a rational number led to a contradiction. π cannot be rational.

□

4 Constructible Numbers

5 Transcendence

We have learned about irrational numbers already and we have seen some prove that both e and π are irrational numbers and almost all roots. But it turns out that there is a more mysterious class of numbers. Numbers that are way deeper embedded in the dense fabric of the real numbers. I am talking about the transcendental numbers. This chapter begins with a simple definition of transcendental numbers. After that we will see that there are more transcendental numbers than algebraic numbers. In order to show that transcendental numbers actually exist we will look at the concept of approximating a number by a rational number. Doing so we will see that not all numbers can be approximated arbitrarily close by a rational number. Apart from the transcendental numbers. After that we will dive deeper into the rabbit hole of transcendental numbers and show that our old companions e and π are not only irrational but also transcendental. After this incredible journey we will conclude the chapter with some unsolved problems in the realm of transcendental numbers.

5.1 Algebraic and transcendental numbers

We begin with a simple definition of algebraic numbers.

Definition 5.1. An algebraic number ξ of degree n is the solution or the root of the equation:

$$a_n \, \xi^n + a_{n-1} \, \xi^{n-1} + ... + a_1 \, \xi + a_0 = 0 \tag{128}$$

with $a_n, a_{n-1}, ..., a_0 \ \in \mathbb{Z}$ or $a_n, a_{n-1}, ..., a_0 \ \in \mathbb{Q}$. Both definitions for the coefficients are equivalent. If the coefficients in 128 are rational, one only has to multiply the equation through with the smallest common denominator of all coefficients. This way we will get integer coefficients again. A number that is not algebraic - and therefore not a solution to equation 128 is called a **transcendental number**.

Let's have a look at some simple algebraic numbers. The easiest example is our good old friend, $\sqrt{2}$. It can be expressed as the root of the equation

$$x^2 - 2 = 0 \tag{129}$$

We can therefore conclude that $\sqrt{2}$ is an algebraic number of degree 2. As we will see later, there are no algebraic equations that have e and π as solutions. In the latter this was a prove that squaring the circle is indeed impossible - a thousand year old problem. So we see that not all irrational numbers are alike. There seem to be numbers that are "more irrational" than others. First we learned to differentiate between rational numbers and irrational numbers and now we learn that even the irrational numbers have subcategories: algebraic and transcendental. In our normal day to day we maximally deal with algebraic irrationals. But as we will see in the next section, there are way more transcendental numbers than algebraic ones. A whole new universe is unfolding in front of us.

5.2 Countable or not - the age old question

In the first chapter we have shown that the set of rational numbers is countable whereas on the other hand the set of real numbers between 0 and 1 is not countable. Therefore we have

two types of infinity: the countable and the uncountable infinity. The question we may ask ourselves now is: What makes the real numbers uncountable? The answer is simple - it's the transcendental numbers. In this section we will show that the set of algebraic numbers is countable which makes the set of transcendental numbers uncountable. This means that although we have infinitely many rationals, algebraic or transcendental numbers, there exist more of the transcendental numbers than of the algebraic or rational ones. So let's just jump right into it!

To prove that the algebraic numbers indeed form a countable set, we first have to make a little detour back into the world of bijective functions and countability.

5.2.1 Countable unions of countable sets

We have looked at different types of sets and investigated, if they are countable or not. In this section we will show that even infinite unions of countable sets form a countable set. But before we can do that, we have to have a look at the composition of bijective functions.

Theorem 5.1. Let $f : A \longrightarrow B$ and $g : B \longrightarrow C$ be bijective functions. Then $g \circ f : A \longrightarrow C$ is bijective.

Proof. To show the correctness of the theorem, we have to show that $g \circ f$ is both surjective and injective. We start with showing that it is surjective. We have to show:

$$\forall\, y \in C\ \exists\ x \in A\ :\ g(f(x)) = y \tag{130}$$

We start with choosing an arbitrary $y \in C$. Since $g : B \longrightarrow C$ is bijective, it is also surjective. Therefore $\exists\, b \in B\ :\ g(b) = y$. On the other hand $b \in B$ and $f : A \longrightarrow B$ is bijective, so for this b there must exist a $x \in A$ such that $f(x) = b$. Therefore we can conclude, that indeed $\exists\, x \in A :\ g(f(x)) = y$ and $g(f(x))$ is surjective.

Now we show that $g(f(x))$ is injective. We need to show that:

$$g(f(x)) = g(f(y)) \Rightarrow\ x = y \quad \forall x, y \in A \tag{131}$$

Start with $g(f(x)) = g(f(y))$. Since $g : B \longrightarrow C$ is bijective, we can conclude that $f(x) = f(y)$. And since $f : A \longrightarrow B$ is bijective as well, we get $x = y$. So the composition is injective. Together with the surjectivity we now know that the composition of two bijective functions is bijective again. This we can now apply to show a useful theorem for countable sets.

□

Theorem 5.2. Let A be an infinite set. A is countable if there exists an injective function $f : A \longrightarrow \mathbb{N}$.

So to show that a set A is countable, it is sufficient to construct an injective function.

Proof. Let $f : A \longrightarrow \mathbb{N}$ be an injective function. Then there must exist a $B \subseteq \mathbb{N}$ such that $f : A \longrightarrow B$ is surjective. Since B is a subset of the natural numbers, it must be

countable. Therefore a bijection $g : B \longrightarrow \mathbb{N}$ must exit. Since both f and g are bijective functions, the composition of both $g \circ f : A \longrightarrow \mathbb{N}$ is bijective as well and creates a one-to-one correspondence between the elements of A and the natural numbers. □

Now we have the tools to show that even the cartesian product of the natural numbers is countable.

Theorem 5.3. The set $\mathbb{N} \times \mathbb{N}$ is countable.

Proof. We will use the previous theorem and construct a injection.

$$f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \ with \ f(m,n) = 2^m 3^n \tag{132}$$

Because every number has a unique prime factorization this function must be injective. So we successfully constructed an injective function from the cross product of the positive integers onto the positive integers. Therefore $\mathbb{N} \times \mathbb{N}$ is countable. □

Now we have all the tools to tackle the original problem of this section:

Theorem 5.4. A countable union of countable sets is countable.

Proof. Let

$$\{A_i\}_{i \in \mathbb{N}} \tag{133}$$

a countable set of countable sets A_i and first assume that those sets are disjoint $A_j \cap A_k = \emptyset$ for $j \neq k$. For every A_i there exists a bijection $f_i : \mathbb{N} \longrightarrow A_i$. Now let

$$A = \bigcup_{i \in \mathbb{N}} A_i \tag{134}$$

We construct a function

$$f : \mathbb{N} \times \mathbb{N} \longrightarrow A \tag{135}$$

$$f(m,n) = f_m(n) \tag{136}$$

Since we have shown that $\mathbb{N} \times \mathbb{N}$ is countable, a bijection onto A would prove A to be countable. So now we just have to show that f is bijective.

We start with surjectivity. To do so we have to show the following:

$$\forall\, x \ \in \ A \ \exists \ x \ \in \ \mathbb{N} \times \mathbb{N} \ : \ f(m,n) = x \tag{137}$$

Let $x \in A$ be arbitrary. Since $A = \bigcup_{i \in \mathbb{N}} A_i \ \Rightarrow \exists\, m \in \mathbb{N} : x \in A_m$. Since A_m is countable, there exists the a bijection f_m with some $n \in \mathbb{N}$ such that $f_m(n) = f(m,n) = x$. So f is surjective.

Now to the injective part. We have to show that:

$$f(m,n) = f(p,q) \Rightarrow \ m = p \ and \ n = q \ \ \forall m,n,p,q \in \mathbb{N} \times \mathbb{N} \tag{138}$$

So assume $f(m,n) = f(p,q)$. This means $f_m(n) = f_p(q)$. We see that $f_m(n) \in A_m$ and $f_p(q) \in A_p$. Since all the sets are disjoint, neither $f_m(n)$ nor $f_p(q)$ can be in another set. So we must conclude that $m = p$. Now we remain with showing that $n = q$. We know that $m = p$ so we can write $f_m(n) = f_m(q)$. This function is bijective, therefore injective and therefore $n = q$ has to be true. So f is also injective. And combining everything we found that f is bijective. Now what happens if the sets A_i are not disjoint? The prove still works. We just have to define $A'_1 = A_1$ and for $i \geq 2$

$$A'_i = A_i - \bigcup_{j=1}^{i-1} A_j \tag{139}$$

Then all A'_i are disjoint, but the the union is still the same:

$$\bigcup_{i \in \mathbb{N}} A_i = \bigcup_{i \in \mathbb{N}} A'_i \tag{140}$$

□

5.2.2 Algebraic Numbers are countable

Theorem 5.5. The set of algebraic numbers is countable.

Proof. Every algebraic number corresponds to at least one algebraic equation of degree N. So if we can show that the set of algebraic equations is countable, we could conclude that the set algebraic numbers also is. We start by defining the rank of an algebraic equation as:

$$N = n + \mid a_n \mid + \mid a_{n-1} \mid + ... + \mid a_0 \mid \tag{141}$$

The smallest rank an algebraic equation can have is $N = 2$. The simplest definition of an algebraic number through an algebraic equation would be:

$$x - 1 = 0 \tag{142}$$

The algebraic number defined through this equation would be $x = 1$ and the rank is $N = 2$. Since an algebraic equation of rank N only has a finite amount of coefficients, there is also only finitely many possible combinations of coefficients that result in that rank N. So the equations of rank N could be listed up like:

$$E_{N,1}, E_{N,2}, ..., E_{N,k_N} \tag{143}$$

For each rank N there are k_N equations. We can list up the equations for all of the ranks:

$$E_{N=2,1}, E_{2,2}, ..., E_{2,k_N}, ..., E_{N,1}, E_{N,2}, ..., E_{N,k_N}, ... \tag{144}$$

We can see this list of equations as a set including sets. For each rank we have a finite set of equations and all of those sets together form the set of equations for each rank which an algebraic equation can have. So we have the set of algebraic equations:

$$A = \{\{E_{2,1}, E_{2,2}, ..., E_{2,k_N}\}, ..., \{E_{N,1}, E_{N,2}, ..., E_{N,k_N}\}, ...\} \tag{145}$$

Each subset of A is finite and therefore countable. Each subset in A also corresponds to a rank N so each set just corresponds to a natural number - starting with 2. Therefore we have a countable union of countable sets which in turn is again countable. So we figured out that the set of algebraic equations is countable. Since each algebraic number corresponds to at least one of the algebraic equations we can conclude that the set of algebraic numbers is countable. □

With this we can easily prove the next theorem.

Theorem 5.6. The set of transcendental numbers is not countable.

Proof. We know the real numbers are not countable. We know the real numbers consist of algebraic numbers and transcendental numbers. As we have just proven, the set of algebraic numbers is countable. Therefore the set of transcendental numbers has to be uncountable. □

5.3 The algebraic closure of algebraic numbers

We have seen that algebraic numbers are roots of polynomials with integer or rational coefficients. But what happens if we make the coefficients algebraic as well? Is it possible to construct a transcendental number by making it the root of a polynomial with algebraic coefficients? This is the question that we will answer in this section and I can already tell you the answer: it is not possible. Algebraic numbers have a feature which we call the algebraic closure. Every root of a polynom with algebraic coefficients is indeed an algebraic number. This is expressed in the theorem:

Theorem 5.7. Let λ be the root of a polynom with algebraic coefficients:

$$a_n\lambda^n + a_{n-1}\lambda^{n-1} + ... + a_1\lambda + a_0 = 0 \tag{146}$$

5.4 Approximation by rationals

The approximation of a number by rational numbers is the central concept in understanding transcendental numbers and their difference to algebraic irrational numbers. First we begin with a simple definition.

Definition 5.2. A number $\xi \in \mathbb{R}$ can be approximated by rationals to order n if there exists a $K(\xi)$ such that

$$| \frac{p}{q} - \xi | < \frac{K}{q^n} \tag{147}$$

has infinitely many solutions $\frac{p}{q}$.

Not all numbers can be approximated to the same order by rational numbers. Rational numbers themselves only can be approximated to order 1 and no higher. Algebraic numbers of degree n can be approximated to order n. This means that $\sqrt{2}$ is approximable by rationals to order 2. And transcendental numbers are very special. They can be approximated by rationals to any high order. As high as you please. This means a transcendental number can be approximated to an arbitrary order other than other irrational numbers.

Theorem 5.8. Rational numbers can be approximated by rationals to order 1 and no higher order.

Proof. We prove by contradiction. We assume that rationals can be approximated by rationals to order 2. So for $\xi \in \mathbb{Q}$ with $\xi = \frac{a}{b}$ being approximated by a rational $r = \frac{p}{q}$ with $r \neq \xi$ the inequality

$$| \frac{p}{q} - \frac{a}{b} | \leq \frac{K}{q^2} \tag{148}$$

has an infinity of solutions. But at the same time we can write the difference as:

$$| \frac{p}{q} - \frac{a}{b} | \geq \frac{| pb - aq |}{| bq |} \geq \frac{1}{| bq |} \geq \frac{1}{bq} \tag{149}$$

Together with equation 148 we get the following inequality:

$$\frac{1}{bq} \leq | \frac{p}{q} - \frac{a}{b} | \leq \frac{K}{q^2} \tag{150}$$

So for the denominator q we get the following condition:

$$\frac{1}{bq} < \frac{K}{q^2} \Rightarrow Kbq > q^2 \Rightarrow q < Kb \tag{151}$$

So in order for equation 148 to be true, q needs to be smaller than the product Kb. This means that the denominator q of the fraction $\frac{p}{q}$ is bounded by a finite number and can therefore not grow arbitrarily big. This in turn means that $\frac{p}{q}$ cannot get arbitrarily small. So there cannot be an infinite amount of solutions to the inequality 148. Therefore a rational number cannot be approximated by rationals to order 2 or any higher order. □

So a rational can be approximated by a rational to order 1. This sounds quite logical. In the next step we will show the second statement: That algebraic numbers of degree n are approximable to order n, but no higher order.

5.5 The Liouville Theorem

Let's jump right into the theorem:

Theorem 5.9. An algebraic number ξ of degree n can only be approximated to order n and no higher order.

Proof. We prove this theorem similar to before when we showed that a rational can only be approximated to order 1 and no higher order. We will assume that ξ can be approximated

to order n+1. This means that the inequality

$$| \frac{p}{q} - \xi | \leq \frac{K}{q^{n+1}} \tag{152}$$

has an infinite amount of solutions. Now let ξ be a root of the function

$$f(\xi) = a_n \xi^n + a_{n-1} \xi^{n-1} + ... + a_0 = 0 \tag{153}$$

For the function $f(x)$ choose a small interval $[\xi - 1, \xi + 1]$. In this interval the function is bounded by a constant M:

$$\exists\, M \,\forall\, x \,\in\, [\xi - 1, \xi + 1] : | f'(x) | < M \tag{154}$$

Now let's approximate ξ with some rational $\frac{p}{q}$, such that $\frac{p}{q}$ is in the interval $[\xi - 1, \xi + 1]$ and not a root of equation 153, so $f(\frac{p}{q}) \neq 0$. Let's take a look at $| f(\frac{p}{q}) |$ specifically:

$$| f(\frac{p}{q}) | = | a_n \frac{p^n}{q^n} + a_{n-1} \frac{p^{n-1}}{q^{n-1}} + ... + a_0 | = \tag{155}$$

$$\tag{156}$$

$$\frac{1}{| q^n |} \Big(| a_n p^n + a_{n-1} p^{n-1} q + ... + a_0 q^n | \Big) = \tag{157}$$

$$\tag{158}$$

$$\frac{| a_n p^n + a_{n-1} p^{n-1} q + ... + a_0 q^n |}{| q^n |} \geq \frac{1}{q^n} \tag{159}$$

$$\tag{160}$$

Now on the other hand we have the following equation:

$$| f(\frac{p}{q}) | = | f(\frac{p}{q}) - f(\xi) | \tag{161}$$

because $f(\xi) = 0$. According to the mean value theorem we can find some x between ξ and $\frac{p}{q}$ such that:

$$f'(x) = \frac{f(\frac{p}{q}) - f(\xi)}{\frac{p}{q} - \xi} \tag{162}$$

So rearranging the terms gives us:

$$f(\frac{p}{q}) - f(\xi) = (\frac{p}{q} - \xi) \cdot f'(x) \tag{163}$$

This we can now plug into equation 161:

$$| f(\frac{p}{q}) | = | f(\frac{p}{q}) - f(\xi) | = | \frac{p}{q} - \xi | \cdot | f'(x) | \tag{164}$$

With equation 154 we get that for an x between $\frac{p}{q}$ and ξ:

$$| \frac{p}{q} - \xi | \cdot | f'(x) | < M \cdot | \frac{p}{q} - \xi | \tag{165}$$

On the other hand we assumed in the beginning that

$$| \frac{p}{q} - \xi | \leq \frac{K}{q^{n+1}} \tag{166}$$

has infinitely many solutions. So we can plug this into equation 165 and get:

$$M \cdot | \frac{p}{q} - \xi | < M \frac{K}{q^{n+1}} \tag{167}$$

Let's combine all of this with equation 155:

$$\frac{1}{q^n} < | f(\frac{p}{q}) | = | f(\frac{p}{q}) - f(\xi) | = | \frac{p}{q} - \xi | \cdot | f'(x) | < \frac{KM}{q^{n+1}} \tag{168}$$

So in short we can write:

$$\frac{1}{q^n} < \frac{KM}{q^{n+1}} \tag{169}$$

Rearranging the terms to get an equation for q gives us:

$$q < KM \tag{170}$$

Both K and M are finite numbers depending on ξ, therefore they act as an upper bound to the denominator q. This means that q cannot grow arbitrarily big and therefore $\frac{p}{q}$ cannot grow arbitrarily small. We can conclude: if ξ is an algebraic number of degree n, then equation 152 cannot have an infinity of solutions. It can therefore not be approximated to order n+1 or any higher order. □

5.6 The first transcendental number

With the theorem of Liouville we are now able to construct the first transcendental number:

$$\xi = \frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \frac{1}{10^{3!}} + ... + \frac{1}{10^{n!}} + ... = \sum_{n=1}^{\infty} \frac{1}{10^{n!}} \tag{171}$$

We will show now that this number can be approximated to any degree we wish, no matter how high. This means it cannot be algebraic according to the Liouville Theorem and therefore must be transcendental.

Proof. Define ξ_n as the sum

$$\xi_n := \sum_{k=1}^{n} \frac{1}{10^{k!}} = \frac{p}{10^{n!}} \tag{172}$$

because the finite sum will have a denominator of $10^{n!}$ by adding up all the bigger fractions. Assume now that ξ_n is algebraic of degree N, meaning it cannot be approximated to a degree higher than N. This means that

$$| \frac{p}{q} - \xi | < \frac{1}{q^{N+1}} \tag{173}$$

does not have an infinity of solutions. We choose n such that $n > N$. Then we can write:

$$| \xi_n - \xi | = \frac{1}{10^{(n+1)!}} + \frac{1}{10^{(n+2)!}} + \frac{1}{10^{(n+3)!}} + ... = \tag{174}$$

$$\tag{175}$$

$$\frac{1}{10^{(n+1)!}} \Big(1 + \frac{1}{(10^{(n+1)!})^{(n+1)}} + \frac{1}{(10^{(n+1)!})^{(n+2)}} \Big) \tag{176}$$

$$\tag{177}$$

$$\leq 2 \cdot 10^{-(n+1)!} < 2 \cdot 10^{-(N+1)} \tag{178}$$

But there are infinitely many ξ_n that satisfy the inequality

$$| \xi_n - \xi | < 2 \cdot 10^{-(N+1)} \tag{179}$$

for arbitrarily big N, so ξ can be approximated to an arbitrary order N. Therefore ξ must be transcendental. □

Theorem 6.1. This is a theorem.

Proposition 6.2. This is a proposition.

Principle 6.3. This is a principle.

References