Introductory Number Theory. Basic definitions and theorems

Leopold Kronecker () famously said “God created the natural numbers. All else is the work of man.” Leaving aside the slight male chauvinism of the saying (nowadays we might say "all else is the work of humans"), what he meant is that the starting point of mathematics are the natural numbers 1, 2, 3, . . . ; those are God-given, we don’t question them. More precisely, natural numbers are the primitive, undefined, objects of mathematics. They are the God-given bricks out which we humans build the magnificent building of mathematics. Well, Kronecker’s view needs some modifications. In the first place, geometry is a very important part of mathematics, and the primitive objects of that part of mathematics are not numbers but points and lines. Moreover, there are parts of mathematics that do not even deal with numbers, at least not directly. In contemporary mathematics, the primitive objects are sets and classes, and the natural numbers are constructed from these objects. While this is very interesting, it is not very illuminating. It doesn’t give you a better feeling for the natural numbers than you might already have. So we will be Kroneckerians, the natural numbers are God’s gift; they are here, they always were here; let’s use them.

But let’s use them carefully and respectfully! Incidentally, the vast majority of mathematicians are Kroneckerians.

We might however ask what are this objects? What is the number 3? (for example). One thing to keep in mind here is that in mathematics what an object is, is a matter of profound indifference. The question “what is 3?” may be of great philosophical interest. What is 3 really? One can say it is the property shared by all sets of 3 elements, but this is sort of circular. The mathematical answer to the question, however, is who cares. What matters is not what an object is, but what properties it has, what you can do with it. This statement has to be slightly modified; you have to know that there is such an object. If we are dealing with primitive objects of some theory (like the natural numbers for us), the basic properties of these objects (called axioms) have to be consistent. Non primitive objects, as the rational numbers, for example, have to be constructed. Otherwise, the duck test applies: “If it quacks like a duck, and walks like a duck; it is a duck.”

Concentrating on our now best friends for life, the natural numbers, we are not going to ask them who or what they are. But we need to know their properties so we know exactly what we can do with them. The Italian mathematician Giuseppe Peano () came up with a set of five axioms that totally characterize the natural numbers. I’ll present them in a somewhat more modern version suitable for this course.

The set \( \mathbb{N} \) of natural numbers is totally characterized by the following properties:

**Peano 1.** \( \mathbb{N} \) contains an object denoted by 1. (Sometimes stated as “1 is a natural number.”)

**Peano 2.** There is a function called “successor of” from \( \mathbb{N} \) to \( \mathbb{N} \); this means that one assigns to every element \( n \in \mathbb{N} \), another element \( n' \in \mathbb{N} \) called the successor of \( n \).

**Peano 3.** If two elements have the same successor, they are equal. In symbols: If \( n, m \in \mathbb{N} \) and \( n' = m' \), then \( n = m \).

**Peano 4.** 1 is not the successor of any element of \( \mathbb{N} \). Or, for every \( n \in \mathbb{N} \), \( n' \neq 1 \).

**Peano 5.** If \( S \) is a set of natural numbers, if \( 1 \in S \), if for every \( n \in S \) it is also true that \( n' \in S \), then \( S \) is the set of all natural numbers. In symbols: If \( S \subset \mathbb{N} \), if \( 1 \in S \), if \( n \in S \Rightarrow n' \in S \), then \( S = \mathbb{N} \). This is the mathematical induction axiom.

It turns out these axioms characterize the natural numbers completely. Like the seed of an oak tree encapsulates the full grown oak, they encapsulate all the properties of the natural numbers; the known ones, the ones to be known, the ones we will perhaps never know.

At first glance that hardly seems possible. Yes, we know that in our usual interpretation with the successor of \( n \) being the next number after \( n \) all these properties hold. But by simply considering the axioms, we do not even know that there is anything in that set \( \mathbb{N} \) other than 1. Yet we know; there is at least another element, namely the successor of 1 which is traditionally denoted by 2. So 2=1’. But now we need a successor of 2. Could we just say 2 is its own successor? So 1’ = 2, 2’ = 2, and we are done. NO. Because then 1’ = 2’ and by Peano 3, 1 = 2; which it isn’t. So we need a third element, lets denote it by the symbol 3, and 2’ = 3. Continuing this way we see that \( \mathbb{N} \)
must actually be an infinite set for the Peano axioms to hold. I don’t want to get too involved with this, I’ll just make the following remarks.

1. Any set \( \mathbb{N} \) satisfying the Peano axioms can serve as set of natural numbers.

2. One can now define the usual operations for natural numbers and prove their properties. As an example, here is how on defines addition.

   (a) Step 1. If \( n \in \mathbb{N} \), we define \( n + 1 = n' \).

   (b) Step 2. Let \( n \in \mathbb{N} \). Assuming \( n + m \) defined for some \( m \in \mathbb{N} \), we define \( n + m' = (n + m)' \).

   (c) Step 3. Verification that now \( n + m \) is defined for all \( m \in \mathbb{N} \), given \( n \in \mathbb{N} \). This is done by induction: Let

   \[ S = \{ m \in \mathbb{N} : n + m \text{ is defined} \}. \]

   Then \( 1 \in S \) by Step 1. If \( m \in S \), then \( m' \in S \) by step 2. Thus, by Peano 5, \( S = \mathbb{N} \), meaning that \( n + m \) is defined for all \( m \in \mathbb{N} \)

But this was a highly asymmetrical definition, it is absolutely not clear (I think) why \( n + m = m + n \). So we need to prove this now. Again, Peano 5 does the trick. But this would take us too far. One also defines \( n \cdot m \) for \( n, m \in \mathbb{N} \) and eventually proves the usual properties of these operations.

3. One defines \( n < m \) for \( n, m \in \mathbb{N} \) by \( n < m \) if and only if \( m = n + a \) for some \( a \in \mathbb{N} \).

4. With \( \mathbb{N} \) defined, one now constructs the set of all integers \( \mathbb{Z} \), defines its operations, proves the properties of these operations. Next one constructs the set of rational numbers \( \mathbb{Q} \), then the set of reals \( \mathbb{R} \), the complex numbers \( \mathbb{C} \). And this is the point where we start.

In this course, a number will always be an integer, except if otherwise explicitly identified.

**Definition 1** Let \( d, m \) be integers, \( d \neq 0 \). We say \( d \) divides \( m \) iff there exists an integer \( k \) such that \( m = dk \). If \( d \) divides \( m \), we write \( d | m \).

**Theorem 1**

1. If \( n \neq 0 \) is an integer, then \( n|n \).

2. \( 1|n \) for all integers \( n \).

3. Every integer \( n \neq 0 \) divides 0.

4. \( m|n \) if and only if \( m \) divides \( n \), if and only if \( -m|n \).

5. If \( m|n \) and \( n \neq 0 \), then \( |m| \leq |n| \).

6. If \( \ell, m, n \) are integers, \( \ell \neq 0 \), \( m \neq 0 \), if \( \ell|m \) and \( m|n \), then \( \ell|n \).

7. If \( n|1 \), then \( n = 1 \) or \( n = -1 \).

8. If \( m|n \) and \( n|m \), then \( n = m \) or \( n = -m \).

9. If \( n|a \) and \( n|b \), then \( n|(a + b) \) and \( n|(a - b) \).

10. If \( n|a \) and \( m|b \), then \( nm|ab \). In particular, if \( n|a \), then \( n^k|a^k \) for \( k = 1, 2, \ldots \).

**Proof.**

1. Let \( n \in \mathbb{N} \), \( n \neq 0 \). Then \( n = 1 \cdot n \), proving \( n|n \).

2. \( n = 1 \cdot n \) for all \( n \).

3. If \( n \neq 0 \), then \( 0 = n \cdot 0 \), proving \( n|0 \).

4. If \( n = mk \), then \( n = (-m)(-k) \) proving \( -m|n \), and \( -n = m(-k) \), proving \( m | -n \). This proves that \( m|n \) implies \( -m|n \) and \( m| -n \). The converse proofs are identical.
5. Assume \( m|n, n \neq 0 \). Then \( n = km, k \neq 0 \neq m \). Then \( |k| \geq 1 \), hence \( |n| = |m||k| \geq |m| \).
6. If \( \ell|m \), then \( m = k\ell \) for some integer \( k \); if \( m|n \) then \( n = jm \) for some \( j \); thus \( n = (jk)\ell \), hence \( \ell|n \).
7. If \( n1 \), then \( |n| \leq 1 \). The only non zero integers satisfying \( |N| \leq 1 \) are \( 1 \) and \( -1 \).
8. If \( m|n \) and \( n|m \), then \( |m| \leq |n| \) and \( |m| \leq |n| \), hence \( |m| = |n| \), hence \( m = \pm n \).
9. Assume \( n|a, n|b \). Then \( a = kn, b = jn \) for some \( k,j \in \mathbb{Z} \); thus \( a + b = (k + j)n \) and \( n|a + b \). Similarly for \( a - b \).
10. If \( a = kn, b = jm \), then \( ab = (kj)(nm) \).

The division algorithm. An Archimedean lemma.

Lemma 2 Let \( n \in \mathbb{Z} \) and \( d \in \mathbb{N} \). There exists a unique \( q \in \mathbb{Z} \) such that \( qd \leq n < (q + 1)d \).

Proof. Case 1 \( n \geq 0 \). Let \( S \) be the set of all integers \( k \geq 1 \) such that \( (k - 1)d \leq n \). Clearly \( 1 \in S \) because \( n \geq 0 \). If \( k \in S \) then taking \( q = k - 1 \) we have \( qd \leq n \); The non-existence of \( q \) with \( qd \leq n < (q + 1)d \) would imply \( (q + 1)d \leq n \), hence \( kd \leq n \) proving \( k + 1 \in S \). Thus \( S = \mathbb{N} \); all natural numbers are in \( S \). This is nonsense! That would mean \( n + 1 \in S \), hence \( (n + 1)d \leq n \), which is ridiculous.

Case 2. \( n < 0 \). By what we proved, there exists \( q \in \mathbb{Z} \) such that \( qd \leq -n < (q + 1)d \). Then \( (-q - 1)d < n \leq (-q)d \).
If \( n \neq -qd \), then we have it; \((-q - 1)d < -n < (-qd)\) implies \((-q - 1)d \leq -n < -qd \). If \( n = -qd \), then \((-q)d \leq n < (-q + 1)d \), and we are also done.

Theorem 3 Let \( n,d \) be integers; assume \( d \neq 0 \). There exist unique integers \( q,r \) such that \( 0 \leq r < |d| \) and \( n = dq + r \).

Proof. Existence. We assume first that \( d > 0 \). By Lemma 2, there is an integer \( q \) such that \( qd \leq n < (q + 1)d \). This \( q \) is our \( q \). We set \( r = n - qd \) and we are done; clearly \( 0 \leq r < d \) and \( n = dq + r \). Assume next that \( d < 0 \). Then, by what was proved, there exist \( q,r \), \( 0 \leq r < -d = |d| \) such that \( n = q(-d) + r \). Then \( n = (-q)d + r \), and we are done.

Uniqueness. Assume for some \( n,d \) there exist \( q,r,q',r' \) such that \( 0 \leq r,r' < |d| \) and \( dq + r = n = dq' + r' \). Then \( dq + r = dq' + r' \), thus \( r - r' = d(q' - q) \). This implies that \( d|d - r' \), thus either \( r = r' = 0 \) or \( |d| \leq |r - r'| \). The latter is impossible; one easily (?) sees that \( 0 \leq r < |d|, 0 \leq r' < |d| \) implies \( |r - r'| < |d| \). Thus \( r = r' = 0 \); i.e., \( r = r' \). But then \( d(q - q') = 0 \), thus also \( q = q' \). Uniqueness is proved.
One calls \( q \) the quotient, \( r \) the remainder of dividing \( n \) by \( d \). We see that \( n \) is divisible by \( d \) if and only if the division of \( n \) by \( d \) has remainder 0.