Number Theory: Part 1

Number theory refers to the study of integers and their properties. Many of the basic concepts of number theory are fundamental to computer science. In this series of lectures, we will cover the concepts of divisibility, modular arithmetic, prime numbers, greatest common divisors, and basic encryption. We begin with the concept of division, which forms the bases of our topic on Number theory.

From now on we will need to be clear when we refer to the natural numbers, $\mathbb{N}$, if we are *including* 0 or not. Most number theorists do **not** include 0, however you may have noticed that depending on where you look, sometimes 0 is included in $\mathbb{N}$. From now on, we assume that $\mathbb{N}$ does **not** include 0, unless we state otherwise.

1 Division

When we are dealing with integers, the symbol for division refers to *integer* division. For example, we say that 2 divides 4 but that 2 does *not* divide 3. This is made clear in the following definition:

Definition. *If a and b are integers and $a \neq 0$, we say that a divides b if an integer c exists where $b = ac$. Thus a is a factor of b and b is a multiple of a.*

For example, since $3|6$, we say 6 is a multiple of 3.

We have the following facts regarding division, which are quite natural. We will work through the proof of just the last one:

Facts:

1. if $a|b$ and $b|c$ then $a|c$.
   For example, $2|6$ and $6|18$ so $2|18$.
2. if $a|b$ and $a|c$ then $a|(b+c)$.
   For example, since $3|6$ and $3|9$ then $3|15$.
3. if $a|b$ then $a|(bd)$ for all integers d.
   For example, since $3|9$ then $3|9(4)$ and $3|9(5)$ etc.

The proof of (3) is straight from the definition of division. If $a|b$ then there exists an integer c such that $ac = b$. Multiply both sides by d and group the cd together as one integer, and you get $a(cd) = bd$. This shows that a divides bd.

If we combine facts (2) and (3) we have the following theorem:

Theorem 1. *Let a, b, c be integers where $a|b$ and $a|c$. Then $a|(mb+nc)$ whenever m and n are integers.*

1.1 Division Algorithm

The following Division theorem is due to Euclid and is most likely familiar. When an integer is divided by a positive integer, there is a quotient and a remainder. What is important in the following theorem is that the integers q and r are **unique**.

Theorem 2. *The Division Algorithm states that when n, d are integers where $d \neq 0$ then there are* ***unique*** *integers q and r such that*

$$n = q \cdot d + r$$

where $0 \leq r < |d|$. The integer r is the remainder and the integer q is the quotient.

Examples

1. For $n = 17$ and $d = 5$ we have the *unique* integers $r = 2$ and $q = 3$:

$$17 = 3 \cdot 5 + 2$$

2. For $n = 17$ and $d = 5$, note that the equation $17 = 2 \cdot 5 + 7$ is **not** an example of the division algorithm because the "remainder" 7 is not less than $d = 5$. The $q = 3$ and $r = 2$ found above are the *unique* solutions to the division algorithm.

3. For $n = 5$ and $d = 7$ we have the *unique* integers $r = 5$ and $q = 0$:

$$5 = 7(0) + 5$$

2 Modular Arithmetic

Very often we care only about the remainder of an integer when it is divided by another. In this section, we introduce **modular arithmetic** and **congruences** which are both based on the remainders as defined in the previous section. The notion of congruences is usually attributed to the German mathematician Carl Friedrich Gauss. He gave us the following definition:

Definition. *If a and b are integers and m is a positive integer, then a is congruent to b modulo m if they have the same remainder when divided by m. We write*

$$a \equiv b \mod m$$

Note that this is the same as saying that m divides $a - b$.

Examples:

1. $17 \equiv 52 \mod 5$ since both numbers have a remainder of 2 when divided by 5. We say that 17 and 52 are **congruent** moduluo 5. We can equivalently see this congruence by noticing that $52 - 17 = 25$ is a multiple of 5.

2. $5 \equiv 2 \mod 3$ since they both have a remainder of 2 when divided by 3. Equivalently, notice that $5 - 2$ is a multiple of 3.

Theorem 3. *Congruences are reflexive, symmetric, and transitive. In other words:*

Reflexive: $a \equiv a \mod m$
Symmetric: $a \equiv b \mod m$ *implies that* $b \equiv a \mod m$
Transitive: $a \equiv b \mod m$ *and* $b \equiv c \mod m$ *implies that* $a \equiv c \mod m$

Examples

1. Since $5 \equiv 2 \mod 3$ and $2 \equiv 14 \mod 3$ then by transitivity, $5 \equiv 14 \mod 3$.

2. Since $9 \equiv 6 \mod 3$, then $6 \equiv 9 \mod 3$.

2.1 Operations involving congruences:

We can manipulate both sides of a congruence similar to the way we work with equations with an equal sign, $=$. For example, we can **add** an integer to both sides of the congruence. Since $2 \equiv 5 \mod 3$ then we can add a 4 to both sides and conclude that $2+4 \equiv 5+4 \mod 3$. Similarly, we could also **multiply** both sides of the congruence with the same number. For example, since $2 \equiv 5 \mod 3$, then by multiplying each side by 4 we conclude that $2 \cdot 4 \equiv 5 \cdot 4 \mod 3$. We can also **add** and **multiply** congruences together, as shown in the following theorem:

Theorem 4. . *If* $a \equiv b \mod m$ *and* $c \equiv d \mod m$ *then*

$$a + c \equiv b + d \mod m$$

$$ac \equiv bd \mod m$$

Proof: Let's look at the formal proof of the first statement from the above theorem. Since $a \equiv b \mod m$ then by definition, we know that m divides $(a - b)$. Similarly, we know that m divides $(c - d)$. Since m divides both of these values, we can add them and m must divide the result. Thus m divides $(a - b) + (c - d)$. After rearranging the terms, we have that m divides $(a + c) - (b + d)$. Thus by the definition of congruence, $(a + c) \equiv (b + d) \mod m$.

Once of the most important facts about congruences, is that we get the same result if we perform the operations first and *then* take the remainder, or if we take the remainder first and *then* perform the operations.

We will start by working through some examples that illustrate this fact, and then state the formal theorem.

Example 1. *Compute* $17 + 45 \mod 3$.

Solution: If we perform the addition *first*, we get $62 \mod 3$, which is 2. If, on the other hand, we carry out the modulus 3 operation *first*, we notice that $17 = 2 \mod 3$ and $45 = 0 \mod 3$, so it is much easier to add $2 + 0 = 2$ and conclude that $17 + 45 = 2 \mod 3$.

Example 2. *Compute* $23 \cdot 41 \mod 5$.

Solution:. Instead of computing $23 \cdot 41$, we can take the modulus first, which makes the multiplication easier. $23 = 3 \mod 5$ and $41 = 1 \mod 5$, thus $23 \cdot 41 = 3 \cdot 1 = 3 \mod 5$.

The property that we are using above to evaluate the sum and multiplication is stated formally in the following theorem:

Theorem 5. *Suppose* m *is a positive integer, and* a *and* b *are integers. Then*

$$(a + b) \mod m = ((a \mod m) + (b \mod m)) \mod m$$

and

$$ab \mod m = ((a \mod m)(b \mod m)) \mod m$$

If the statement of this theorem looks too messy for you, it is really just important to understand how it applies in practice, as we already showed in examples 1 and 2 above.

3 The ring $\mathbb{Z}_n$

We noted above that congruences are **reflexive, symmetric** and **transitive**. Hopefully this reminds you of our lecture on *binary relations* where we defined an **equivalence relation** over a set S as a relation that

had exactly these three properties. Therefore, congruence modulo m over the integers is an equivalence relation.

You may also recall from our material on relations, that equivalence relations over a set can be used to **partition** the elements of that set into **equivalence classes**. As a brief recap, recall that we used the notation $[a]$ to denote the set of elements that were equivalent to the element a.

$$[a] = \{b \in S | (a, b) \in R\}$$

Let's look at an example from our section on relations just to fortify this concept.

Example 3. *Consider the set of integers with the relation congruence modulo 4. What are the equivalence classes?*

Solution: We start with the equivalence class of 0, that is, all elements that are equivalent to 0 under modulo 4, which means they all must have a remainder of 0 when divided by 4. The elements in that set are:

$$[0] = \{0, 4, 8, 12, 16, \ldots\}$$

Recall from our old lecture material that 0 was a defined as a **representative** of this equivalence class. In fact, any element in this set could be used as a representative. For example 8 is also a representative, since the equivalence class of 8 is the same as the equivalence class of 0. This means that $[0] = [8]$, in other words both 0 and 8 are simply representatives of above equivalence class.

Similarly, the equivalence class of 1 is all elements that have the *same* remainder as 1 when they are divided by 4.

$$[1] = \{1, 5, 9, 13, 17, \ldots\}$$

Again we have many possible representatives of this class: $[1] = [13] = [9]$, etc. Continuing, we have two more equivalence classes:

$$[2] = \{2, 6, 10, 14, 18, \ldots\}$$

$$[3] = \{3, 7, 11, 15, 19, \ldots\}$$

Notice that there are *no more* equivalence classes. Any other element in $\mathbb{Z}$ is already contained in one of these 4 classes. Thus these four classes have formed a **partition** of the elements of $\mathbb{Z}$.

Following this example, it is easy to see that we would have a similar set of equivalence classes if we were dealing in a different modulus. For example, in modulo 6, there would be exactly 6 equivalence classes and their natural representatives would be:

$$[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6$$

Similarly, in modulo n, there are exactly n equivalence classes:

$$\{[0]_n, [1]_n, \ldots, [n-1]_n\}$$

The above set of elements is often called the residue class modulo n, or the congruence class modulo n, and is denoted $\mathbb{Z}_n$. Sometimes the notation of the brace brackets is dropped and we write that the set of elements of $\mathbb{Z}_n$ as

$$\{0, 1, 2, 3, \ldots, n-1\}$$

You will likely notice this simplification in different texts and online. It is important to note however, that the above elements each represent an entire *class*. For example, if $n = 9$, the the elements of $\mathbb{Z}_9$ are : $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$. Since each of these elements represents an entire *class*, then we simply think of the element 10 in $\mathbb{Z}_9$ as being equivalent to 1, and similarly, the number 17 in $\mathbb{Z}_9$ is simply the same as the element 8.

We next look at the structure of $\mathbb{Z}_n$ and how to carry out operations in this congruence class.

3.1 Operations on $\mathbb{Z}_n$

We have already seen how to multiply and add in a congruence modulo m, and thus multiplying and adding in the ring $\mathbb{Z}_n$ works in the same way. We can add and multiply elements before and/or after we carry out the modulus operation, and we arrive at the same answer.

For example, suppose $n = 9$ (thus we are in modulus 9), then the ring $\mathbb{Z}_9$ has 9 elements: the equivalence classes $[0], \ldots, [8]$. If we drop the notation of the brace brackets, we could also write that the elements more simply as: $\{0, 1, 2, \ldots, 8\}$, as long as it remains clear that each integer actually represents an entire equivalence class.

Now suppose we want to **add** elements or **multiply** elements of $\mathbb{Z}_9$ together. We do this in exactly the same as with congruences. Since the *elements* themselves are assumed to be the representatives in $\mathbb{Z}_9$, we do not need to write "*mod 9*" after the equation. We can simply write for example:

- $3 + 7 = 1$
- $3 \cdot 9 = 0$
- $12 + 16 = 1$

The figure below shows the result of adding and multiplying the 5 elements of the ring $\mathbb{Z}_5$ and the results:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

3.2 Multiplicative Inverses and Cancelling

We are all quite comfortable with the concept of of **cancelling** and **multiplying by an inverse** when the operations are over the **real numbers**. For example, we learned as children (probably) that in an equation such as

$$2x = 4.6$$

we could *solve* for x by simply multiplying each side by $1/2$. Essentially we were multiplying each side by the **multiplicative inverse** of 2.

The notation for the multiplicative inverse of x is x^{-1} and the inverse is defined in such a way that

$$x \cdot x^{-1} = 1$$

Inverses over the Reals:

Over the real numbers, the definition of this inverse is exactly:

$$x^{-1} = \frac{1}{x}$$

For example, the inverse of 3 is $\frac{1}{3}$ since

$$3 \cdot \frac{1}{3} = 1$$

For equations over the real numbers, multiplicative inverses exist for *all* numbers except 0.

Inverses over the Integers:

If we consider elements belonging to the integers, then only 1 and -1 have inverses. The inverse of 1 is 1 and the inverse of -1 is -1. Suppose we consider the integer 3. There is no other integer that we can multiply with 3 to get a result of 1. Thus 3 does not have an inverse.

Inverses over the ring $\mathbb{Z}_n$

For elements in $\mathbb{Z}_n$, things get a little more complicated. To start things off, let's consider the ring $\mathbb{Z}_{10}$. Note that in this ring, the element 3 has a multiplicative inverse since

$$3 \cdot 7 = 21 = 1 \mod 10$$

However the element 2 does not have a multiplicative inverse. One can verify this by simply checking all possible products with 2 in $\mathbb{Z}_{10}$:

$$2 \cdot 1 = 2, 2 \cdot 2 = 4, 2 \cdot 3 = 6, 2 \cdot 4 = 8, 2 \cdot 5 = 0, 2 \cdot 6 = 2, 2 \cdot 7 = 4, 2 \cdot 8 = 6, 2 \cdot 9 = 8$$

The next theorem specifies exactly when an element in $\mathbb{Z}_n$ has an inverse:

Theorem 6. *If the element $k \in \mathbb{Z}_n$ has the property that the* ***only common divisors*** *between k and n is 1, then k has a multiplicative inverse*

To illustrate this theorem, consider again $\mathbb{Z}_{10}$. We saw that 2 did not have an inverse, and this is confirmed by the fact that 2 and 10 share the common factor 2. The theorem above states that the only elements in $\mathbb{Z}_{10}$ that have inverses will be: $1, 3, 7$ and 9. We can confirm this be finding those inverses:

$$1 \cdot 1 = 1 \mod 10$$

$$3 \cdot 7 = 21 = 1 \mod 10$$

$$7 \cdot 3 = 21 = 1 \mod 10$$

$$9 \cdot 9 = 81 = 1 \mod 10$$

Note that the inverse of 9 is actually 9 itself, since $9(9) = 81 = 1$ in $\mathbb{Z}_{10}$.

Consider the table of multiplications for $\mathbb{Z}_5$ that we saw above. It is copied here. Notice that *each* element other than 0 has a number which when multiplied together with the original element results in 1. Thus each element (other than 0) has an inverse.

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

This generalizes to:

Theorem 7. *For p a prime, every element $x \in \mathbb{Z}_p$ has an inverse.*

When multiplicative inverses exist, we can use them to solve equations just as we normally do in the real numbers.

Example 4. *Solve for x in the equation $4x = 5 \mod 7$.*

Solution: The inverse of 4 in $\mathbb{Z}_7$ is 2 since $4 \cdot 2 = 8 = 1 \mod 7$. Thus we can multiply each side by the inverse of 4:

$$\begin{aligned} 4x &= 5 \mod 7 \\ (2)4x &= (2)5 \mod 7 \\ (2 \cdot 4)x &= (2)5 \mod 7 \\ x &= 10 = 3 \mod 7 \end{aligned}$$

In the second last line, the $(2 \cdot 4) = 1$ and thus it does not appear in the next line. Thus the solution is $x = 3$.

We now turn to the concept of cancelling in $\mathbb{Z}_n$ and show when it is allowed. In general, multiplicative terms **cannot** be cancelled in $\mathbb{Z}_n$. Suppose we have the following equation in $\mathbb{Z}_{15}$:

$$3 \cdot 10 = 3 \cdot 5 \mod 15$$

If we cancel the 3's from each side, then we are left with $10 = 5 \mod 15$, which is *not true.*

For elements that **have** multiplicative inverses, we can cancel them from both sides of the equation.

Theorem 8. *If $k \in \mathbb{Z}_n$ has an inverse, and if $a, b \in \mathbb{Z}_n$ where*

$$k \cdot a = k \cdot b \mod n$$

then we can cancel the k from each side and conclude:

$$a = b \mod n$$

For example, if $5 \cdot 3 = 5 \cdot 21$ in $\mathbb{Z}_6$, then we are allowed to cancel the 3's and conclude that $3 = 21 \mod 6$.