Chapter 3

Number Theory

3.1 The Division Algorithm and The Euclidean Algorithm

Recall that we can divide one integer by another to get a *quotient* and a *remainder*. For example, if we divide 99 by 13, we get a quotient of 7 with a remainder of 8. We can write this as

$$99 = (13)(7) + 8.$$

Try this again with 99 and 11. Notice that

$$99 = (11)(9) + 0.$$

In fact, no matter which two integers we begin with, say a and b, we can always find integers q (the quotient) and r (the remainder) such that

$$a = bq + r, \quad 0 \leq r < |b|.$$

This statement is referred to as *The Division Algorithm*. The reader should try several examples.

Recall now that we say b **divides** a if there is an integer q such that $a = bq$. This falls in line with what the division algorithm tells us, since we can write this as

$$a = bq + 0.$$

Notice then that, given two integers a and b, we can conclude that a divides b if and only if the remainder r guaranteed by the division algorithm is equal to 0. For example, it is clear from above that 11 divides 99, but 13 does not divide 99.

In order to understand the theorems presented later in this chapter, we'll need to understand the notion of the *greatest common divisor* or *gcd*

of two integers. Here's the definition: For two nonzero integers a and b, an integer $d > 0$ is called the **greatest common divisor** of a and b if d is a divisor of a and b and we have $c \leq d$ whenever c is a divisor of a an b. We'll use the notation $gcd(a, b) = d$. What we're really interested in is a way to compute $gcd(a, b)$ for nonzero integers a and b. In many cases, we can just find the answer by brute force. For example, try to find $gcd(12, 3)$, $gcd(18, 10)$, and $gcd(8, 3)$. Then attempt to compute $gcd(2520, 698)$. It is clear from this last example that the brute force approach isn't always convenient. For these cases (and, of course, all other cases) we have the **Euclidean Algorithm**. Let's have a look at how the Euclidean algorithm works by computing $gcd(2520, 698)$. First, we'll use the division algorithm to write

$$2520 = (698)(3) + 426$$

We then apply the division algorithm to the pair of numbers made up of the divisor 698 and the remainder 426 from above:

$$698 = (426)(1) + 272$$

and repeat this process until we get a remainder of 0.

$$426 = (272)(1) + 154$$

$$272 = (154)(1) + 118$$

$$154 = (118)(1) + 36$$

$$118 = (36)(3) + 10$$

$$36 = (10)(3) + 6$$

$$10 = (6)(1) + 4$$

$$6 = (4)(1) + 2$$

$$4 = (2)(2) + 0$$

Once we have a remainder of 0, the Euclidean algorithm then tells us that the last nonzero remainder we encountered is the gcd of the two numbers we began with. That is, $gcd(2520, 698) = 2$. Try the Euclidean algorithm for the other pairs of numbers listed above to make sure that you understand how it works.

The Euclidean Division Algorithm can also be used 'backward" in the following sense. It is a fact, which we will not prove, that given integers n and m with $gcd(m, n) = d$, there are unique integers s and t such that

$$sn + tm = d.$$

We can "undo" the Euclidean Division Algorithm to find the numbers s and t. Consider the following display which uses the algorithm, as we did above:

$$\begin{aligned} 11 &= 1 \cdot 7 + 4 && (3.1)\\ 7 &= 1 \cdot 4 + 3 && (3.2)\\ 4 &= 1 \cdot 3 + 1 && (3.3)\\ 3 &= 3 \cdot 1 + 0 && (3.4) \end{aligned}$$

So, we know that $gcd(11, 7) = 1$. Thus, our fact above guarantees that there are unique integers s and t such that

$$s \cdot 11 + t \cdot 7 = 1.$$

To find s and t, we start be solving equations (3.1) and (3.2) displayed above for their remainders:

$$\begin{aligned} 4 &= 11 - 1 \cdot 7 && (3.5)\\ 3 &= 7 - 1 \cdot 4 && (3.6) \end{aligned}$$

We now substitute equation (3.5) into equation (3.6) to get

$$\begin{aligned} 3 &= 7 - 1 \cdot 4 && (3.7)\\ &= 7 - 1 \cdot (11 - 1 \cdot 7) && (3.8)\\ &= 2 \cdot 7 - 1 \cdot 11 && (3.9) \end{aligned}$$

Finally, we solve equation (3.3) for its remainder and make substitutions using (3.5) and (3.9):

$$\begin{aligned} 1 &= 4 - 1 \cdot 3 && (3.10)\\ &= (11 - 1 \cdot 7) - 1 \cdot (2 \cdot 7 - 1 \cdot 11) && (3.11)\\ &= 2 \cdot 11 - 3 \cdot 7. && (3.12) \end{aligned}$$

That is, we have found that $s = 2$ and $t = -3$. Above, we found that $gcd(2520, 698) = 2$. The reader should attempt to use the Euclidean Division Algorithm backward to find numbers s and t such that

$$s \cdot 2520 + t \cdot 698 = 2.$$

This will require significantly more substitution than our previous example, so practice good bookkeeping!

3.2 Congruences

If you happen to look at someone's time-telling device and see "14:36", do you know what time it is? How about "19:19"? Understanding how to use so-called military time is a good first step in understanding congruences. In fact, all we need to do is divide the number to the left of the colon by 12 and take the remainder: 14 divided by 12 has a remainder of 2, and 19 divided by 12 has a remainder of 7 (hence, the times above are 2:36pm and 7:19pm). In general, if we let n be a positive integer, the two integers a and b are said to be **congruent modulo** n if they have the same remainder when divided by n. In symbols, we write $a \equiv b(mod\ n)$ and we call the integer n the **modulus**. From the examples above, we can see that $14 \equiv 2(mod\ 12)$ and $19 \equiv 7(mod\ 12)$. Can you find a number x such that $121 \equiv x(mod\ 6)$? Can you find a number x such that $0 \leq x \leq 5$ and such that $121 \equiv x(mod\ 6)$? Notice that every positive integer is congruent to one of the integers $1, 2, 3, \ldots, n-1$ modulo n. Here are some important facts that we'll need.

- If $a \equiv c(mod\ n)$ and $b \equiv d(mod\ n)$, then $a \pm b \equiv c \pm d(mod\ n)$ and $ab \equiv cd(mod\ n)$.
- If $a + c \equiv a + d(mod\ n)$, then $c \equiv d(mod\ n)$.
- If $ac \equiv ad(mod\ n)$ and $gcd(a, n) = 1$, then $c \equiv d(mod\ n)$

In plain English, the facts above say the following:

- For any number in the congruence, you can substitute any congruent integer.
- You can add or subtract the same integer on both sides of a congruence.
- You must be a bit careful before dividing both sides of a congruence by an integer.

For the last fact, consider the congruence

$$30 \equiv 6(mod\ 8).$$

Try dividing both sides by 3, and then try dividing both sides by 6. Which of the resulting congruences is true? Why?

3.3 The Integers Modulo n

Recall that when working modulo 3, every integer is congruent to one of the numbers 0, 1, or 2. Therefore, in some sense, there are really only 3 integers modulo 3, since any integer can be replaced by one of the integers 0, 1, or 2. We will use the notation

$$[a]_n = \{x \in \mathbb{Z} : x \equiv a (mod\ n)\}.$$

So, for example,

$$\begin{aligned}[0]_3 &= \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\} \\ [1]_3 &= \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\} \\ [2]_3 &= \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}\end{aligned}$$

Notice that $[0]_3 = [3]_3 = [6]_3 = \cdots$, and that similar equalities hold for $[1]_3$ and $[2]_3$. This shows that the three *congruence classes* displayed above are exhaustive (ie, contain all of the integers). In fact, more generally, for any integer n there are exactly n congruence classes modulo n:

$$[0]_n, [1]_n, \ldots, [n-1]_n.$$

Take a minute to convince yourself of this! We define the **integers modulo** n to be the set

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}.$$

For example, $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$. What we'd like to do is have a way to add and multiply integers modulo n (just like we can add and multiply the usual integers) so that our sums and products are again integers modulo n. Luckily, we can do this in the most obvious possible way:

$$[a]_n + [b]_n = [a+b]_n \qquad \text{and} \qquad [a]_n \cdot [b]_n = [ab]_n.$$

Using these definitions, we can make addition and multiplication tables for any given set $\mathbb{Z}_n$. For example, for $\mathbb{Z}_2$, we have

$+$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[1]_2$
$[1]_2$	$[1]_2$	$[0]_2$

$\cdot$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[0]_2$
$[1]_2$	$[0]_2$	$[1]_2$

The reader should take a moment to construct addition and multiplication tables for $\mathbb{Z}_3$.

One very strange thing sometimes happens when we work modulo n that doesn't happen when we work with the usual integers - it is possible to have two nonzero integers modulo n with product equal to zero modulo

n. For example, consider the element $[2]_4 \in \mathbb{Z}_4$. According to our rules for multiplying integers modulo 4, we have

$$[2]_4 \cdot [2]_4 = [4]_4 = [0]_4.$$

For another example, notice that $[6]_8 \cdot [4]_8 = [0]_8$. Can you come up with a few more of your own?

Now, let's try making a multiplication table for $\mathbb{Z}_6$ so we can determine all elements of $\mathbb{Z}_6$ that have product $[0]_6$. If we do this correctly, we'll see that $[0]_6$, $[2]_6$, $[3]_6$, and $[4]_6$ are all elements of $\mathbb{Z}_6$ that we can multiply be a *nonzero* element of $\mathbb{Z}_6$ to get $[0]_6$. We call these elements of $\mathbb{Z}_6$ **divisors of zero** in $\mathbb{Z}_6$. More generally, if $[a]_n \cdot [b]_n = [0]_n$ and $[b]_n \neq [0]_n$, then we call $[a]_n$ a divisor of zero in $\mathbb{Z}_n$. The reader should take a moment to find all of the divisors of zero in $\mathbb{Z}_n$ for $n = 2, 3, \ldots, 11$. Notice that a pattern begins to emerge - if $gcd(a, n) > 1$, then $[a]_n$ is a divisor of zero in $\mathbb{Z}_n$. Furthermore, every element of $\mathbb{Z}_n$ is either a divisor of zero or not, and the elements that are not divisors of zero are called **units** in $\mathbb{Z}_n$. If we remove all of the divisors of zero from $\mathbb{Z}_n$, then we are left with the set of units in $\mathbb{Z}_n$, which we will denote by $\mathbb{Z}_n^\times$. The reader should note that the units of $\mathbb{Z}_n$ are precisely the elements $[a]_n \in \mathbb{Z}_n$ such that $gcd(a, n) = 1$ (ie, a and n are relatively prime). The theorems of the next section essentially say something important about the units of $\mathbb{Z}_n$.

3.4 Theorems of Euler and Fermat

Before we can investigate the results of Euler and Fermat, we'll need to establish some standard facts and definitions. First, we'll recall that the **Fundamental Theorem of Arithmetic** says that and integer $n > 1$ can be factored uniquely into a product of primes

$$n = p_1^{k_1} p_2^{k_2} \cdots p_j^{k_j}$$

where $p_1 < p_2 < \cdots < p_j$ and the exponents $k_1, k_2, \ldots, k_j$ are all positive. The reader should verify this theorem for several integers (ie, write out the prime factorizations for a bunch of integers).

Now, to motivate Fermat's Little theorem (stated below) let's choose a prime number p and compute some powers of nonnegative integers modulo p. For example, start with $p = 2$ and compute $a, a^2, a^3, \ldots (mod\ 2)$ for $a = 0, 1, 2, \ldots$. Repeat this process for the primes 3, 5, 7, and 11 (it may be useful to put the results of your computations in a table). What we are looking for here are patterns among the various tables one can construct in this way. For our purposes, the pattern that we wish to acknowledge has

to do with the values of

$$a^2(mod\ 3), \qquad a^4(mod\ 5), \qquad a^6(mod\ 7), \qquad a^{10}(mod\ 11)$$

and so on, for $a = 0, 1, 2, 3, \ldots$. Can you see the pattern?

Fermat's Little Theorem. *Let p be a prime number and suppose that a is not divisible by p. Then $a^{p-1} \equiv 1(mod\ p)$.*

To see why a result like this is powerful, consider the following congruence.

$$73^{100} \equiv 1(mod\ 101).$$

If we believe Fermat's Little Theorem, then this congruence is true since 101 is prime and 73 is not divisible by 101. But how would we attempt to verify this congruence if we didn't know the previous theorem? We would have to compute $73^{100} - 1$ and verify that the result is divisible by 101. But $73^{100} - 1$ has 187 digits! Notice further that the prime we are using here is only three digits long. What if we wished to verify the congruence $73^{8675308} \equiv 1(mod\ 8675309)$ without the theorem above? As another example of what Fermat's Little Theorem can do, let's compute

$$3^{32}(mod\ 7).$$

We know that $3^6 \equiv 1(mod\ 7)$. Further, we can use the division algorithm to write $32 = (6)(5) + 2$, so that

$$3^{32} = 3^{6\cdot 5+2} = (3^6)^5 \cdot 3^2 \equiv 1^5 \cdot 3^2 = 9 \equiv 2(mod\ 7).$$

Now, we may be able to handle this with brute force since we can compute $3^{32} = 1853020188851841$, but Fermat's Little Theorem allows us to avoid dealing with such a number. As yet another example of the power of Fermat's Little Theorem, suppose that we want to solve the congruence

$$x^{203} \equiv 4(mod\ 11).$$

Clearly x is not divisible by 11, for otherwise $x^{203} \equiv 0(mod\ 11)$. Using Fermat's Little Theorem, we know that

$$x^{10} \equiv 1(mod\ 11).$$

Raising both sides to the 20th power then gives

$$x^{200} \equiv 1(mod\ 11).$$

Thus,

$$x^{203} = x^{200} \cdot x^3 \equiv x^3(mod\ 11)$$

and solving the original congruence amounts to solving the congruence $x^3 \equiv 4(mod\ 11)$. Now we can just compute $x^3(mod\ 11)$ for $x = 0, 1, \ldots, 10$ to find our solution (which happens to be $x \equiv 5(mod\ 11)$).

One naturally wants to question the validity of a theorem like Fermat's Little Theorem if we replace p by a composite number. That is, is it true that

$$a^{n-1} \equiv 1(mod\ n)$$

for a composite number n that does not divide a? Unfortunately, the answer is no. To get a better idea of what to do in a situation like this, we need to introduce a function that is very important in number theory and algebra, namely **Euler's Phi Function**. If n is a natural number, this function is defined by

$\phi(n) =$ the number of natural numbers less than n that are relatively prime to n.

Euler's Theorem. *If* $gcd(a, n) = 1$*, then* $a^{\phi(n)} \equiv 1(mod\ n)$.

We'll have plenty of opportunity later to deal with this theorem, but for now, it will be worth our while to look deeper into the phi function. The following list of exercises is intended to be an introduction to the phi function from which the reader will have a chance to investigate the phi function and likely derive some of the important properties of the phi function.

1. Compute $\phi(n)$ for $n = 1, \ldots, 20$.

2. Find a pattern for $\phi(n)$ when n is prime.

3. Compute $\phi(2^k)$ for $k = 1, \ldots, 5$. Then repeat these 5 computations for $\phi(3^k)$, $\phi(5^k)$, $\phi(7^k)$, and $\phi(11^k)$. Can you see a general formula for $\phi(p^k)$ where p is a prime number and k is any power of p?

4. Verify that $\phi(4 \cdot 3) = \phi(4) \cdot \phi(3)$, $\phi(25 \cdot 2) = \phi(25) \cdot \phi(2)$, and $\phi(9 \cdot 8) = \phi(9) \cdot \phi(8)$. Then verify that $\phi(3 \cdot 6) \neq \phi(3) \cdot \phi(6)$ and $\phi(2 \cdot 4) \neq \phi(2) \cdot \phi(4)$. Can you figure out, in general, when $\phi(mn) = \phi(m) \cdot \phi(n)$?

5. Find a general formula for $\phi(n)$ for any integer $n > 1$. (Recall that we can write $n = p_1^{k_1} p_2^{k_2} \cdots p_j^{k_j}$. Apply the phi function to both sides of this equation and, using what we've found above, try to "break down" $\phi(p_1^{k_1} p_2^{k_2} \cdots p_j^{k_j})$ as far as you can!)

3.5 General Theory of Number Systems

Consider the number 719. We know that the 9 is in the "ones" place, the 1 is in the "tens" place, and the 7 is in the "hundreds" place. But why, exactly, do these places have these names? Why start with "ones" and then skip to "tens"? The answer is pretty simple – these are the first three nonnegative powers of 10. Notice that we can write

$$719 = 7 \cdot 10^2 + 1 \cdot 10^1 + 9 \cdot 10^0.$$

This number system is known as the **base-10** or **decimal** number system. It uses the ten digits 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9 to say how many objects we have in each named place. That is, 719 means that we have 7 hundreds, 1 ten, and 9 ones. Of course, there is nothing special about using 10 as the base (other than the fact that it is the most familiar to us). We could, for example, us a base of 3 instead. In this case, we would have the digits 0,1, and 2 and we would name the places in each number after the nonnegative powers of 3. To write 719 in base-3 notation, we might start by listing the powers of 3 until we get such a power that is larger than 719:

$$3^0 = 1 \quad 3^1 = 3 \quad 3^2 = 9 \quad 3^3 = 27 \quad 3^4 = 81 \quad 3^5 = 243 \quad 3^6 = 729 \quad .$$

Thus, we see that 3^5 is the largest power of 3 that fits into 719 (twice, in fact) and we can write

$$719 = 2 \cdot 3^5 + 233.$$

Continuing in this fashion, we see that the largest power of 3 that fits into 233 is 3^4, and we can write

$$719 = 2 \cdot 3^5 + 2 \cdot 3^4 + 2 \cdot 3^3 + 1 \cdot 3^2 + 2 \cdot 3^1 + 2 \cdot 3^0.$$

In other words, in base-3 notation we can write 719 as 222122. We will denote this by writing

$$719 = 222122_3.$$

When we intend for the number to be in decimal form, we will not use a subscript. For example, we will write 719 instead of 719_{10}. Note that we can carry out addition of numbers in any base, as long as we follow the rules for that base. For example, $25 = 221_3$ (as the reader should check) and we can add this to $719 = 222122_3$ by "carrying" as long as we remember that $3 = 10_3$, $4 = 11_3$, and $5 = 12_3$. Thus, we get

$$719 + 25 = 222122_3 + 221_3 = 1000120_3.$$

The reader should work this out by hand, and then verify that the addition is correct. That is, convert 1000120_3 back to decimal notation and make sure that the result is 744.

3.5.1 Binary and Hexadecimal

The base-2 number system is called the **binary** number system, and will prove to be important for us down the road. In this system, the only digits are 0 and 1. These binary digits are called "bits", which is just a term created by mashing together the words "binary" and "digits". As practice, the reader should verify the correctness of the following table, which gives the binary representations of the first several decimal numbers. We will omit the subscript of 2 for the binary numbers in this table.

Decimal	Binary
0	0
1	1
2	10
3	11
4	100
5	101
6	110
7	111
8	1000
9	1001
10	1010

Decimal	Binary
11	1011
12	1100
13	1101
14	1110
15	1111
16	10000
17	10001
18	10010
19	10011
20	10100

The base-16 number system is called the **hexadecimal** number system. This number system will be convenient for several reasons, namely because $2^4 = 16$. When working base-16, we run into a bit of a problem with digits. We use the digits $0, \ldots, 9$ as usual, but now we need a way to describe the digits 10, 11, 12, 13, 14, and 15 (and yes, in base-16, these are digits!). To represent these digits without confusing ourselves, we replace them with the letters A,B,C,D,E, and F. That is, A stands for the digit 10, B stands for the digit 11, and so on with F standing for the digit 15. So, for example, let us consider the decimal number 123456. The largest power of 2 that fits into 123456 is 2^{16} so representing this number in binary notation would take up a lot of space! However, we see that the largest power of 16 that fits into 123456 is $16^4 = 65536$. Thus, it is much more efficient to represent this number in base-16. To do so, we proceed as usual to obtain

$$123456 = 1 \cdot 16^4 + E \cdot 16^3 + 2 \cdot 16^2 + 4 \cdot 16^1 + 0 \cdot 16^0.$$

That is, $123456 = 1E240_{16}$. It is also convenient to convert binary numbers directly to hexadecimal numbers. For some examples, we have.

$$110010111011_2 = CBB_{16} \qquad 110101110101111101111101_2 = 6BAFBD_{16}$$

For the first of these examples, separate the binary digits on the left side of each equation into groups of four, starting from the right. So, for the first display, we would have the groups

$$\overbrace{1100}\,\overbrace{1011}\,\overbrace{1011}.$$

If the number of bits is not a multiple of four, then just use what you have remaining for the leftmost group. We now treat each of these groups as a separate binary number, and convert them back to decimal notation:

$$1100_2 = 15 \quad 1011_2 = 11 \quad 1011_2 = 11.$$

Finally, we observe that in hexadecimal notation, the numbers above correspond to C, B, and B, respectively. Hence $110010111011_2 = CBB_{16}$. The reader should now verify the second example above.

3.6 Successive Squaring

The following example can be found in Chapter 16 of the beautiful text [2]. What if you were asked to compute

$$5^{100000000000000}(mod\ 12830603)?$$

By now, we should know better than to try to enter this number into our personal calculator! It turns out that our modulus has prime factorization

$$12830603 = 3571 \cdot 3593$$

so we know that

$$\phi(12830603) = \phi(3571) \cdot \phi(3593) = 3570 \cdot 3592 = 12823440.$$

Now, using Euler's Theorem, we know that

$$5^{12823440} \equiv 1(mod\ 12830603)$$

so we may write

$$\begin{aligned} 5^{100000000000000} &= (5^{12823440})^{7798219} \cdot 5^{6546640} \\ &= 5^{6546640}(mod\ 12830603). \end{aligned}$$

Unfortunately, the number $5^{6546640}$ still has more than four million digits, so we've simplified our problem, but not yet enough for a computer to easily handle. Even worse, some of the ciphers that we will discuss in the next chapter require one to compute $a^k(mod\ m)$ for a, k, and m each

having hundreds of digits! We will attack this problem using the method of successive squaring, which we will now illustrate. To that end, let's consider

$$3^{97}(mod\ 353).$$

You might try to enter 3^{97} in your calculator, but you'll have little success since this number already has nearly fifty digits! It is easy, however, for us to compute that

$$97 = 1100001_2 = 64 + 32 + 1$$

so that

$$3^{97} = 3^{64} \cdot 3^{32} \cdot 3^1.$$

We can now compute this number by squaring the number 3 over and over again, reducing modulo 353 at every step along the way.

$$\begin{aligned}
3 &\equiv 3(mod\ 353) \\
3^2 &\equiv 9(mod\ 353) \\
3^4 &\equiv 9^2 \equiv 81(mod\ 353) \\
3^8 &\equiv 81^2 \equiv 207(mod\ 353) \\
3^{16} &\equiv 207^2 \equiv 136(mod\ 353) \\
3^{32} &\equiv 136^2 \equiv 140(mod\ 353) \\
3^{64} &\equiv 140^2 \equiv 185(mod\ 353)
\end{aligned}$$

Using these computations, we can now make the following substitutions:

$$3^{97} = 3^{64} \cdot 3^{32} \cdot 3^1 \equiv 185 \cdot 140 \cdot 3(mod\ 353).$$

One final reduction of the product $185 \cdot 140 \cdot 3$ modulo 353 gives us our answer, which is 40. For practice, the reader should use this same technique to compute

$$7^{327}(mod\ 853).$$

Bibliography

[1] Beachy, J., Blair, W.: *Abstract Algebra.* 2nd Edition. Waveland Press, Inc. (1996).

[2] Silverman, J.: *A Friendly Introduction to Number Theory.* 3rd Edition. Pearson Prentice Hall (2006).

[3] Eggen, M., Smith, D., St. Andre, R.: *A Transition to Advanced Mathematics.* 7th Edition. Brooks/Cole (2011).