Chapter 5

Number Theory

5.1 Prime Numbers

Any two integers can be multiplied together to produce a new integer. For example, we can multiply the numbers four and five together to produce twenty. In this situation we say that "four divides twenty" and "five divides twenty", and we write $4|20$ and $5|20$. More generally, we say $a|c$ if there is some integer b such that $ab = c$.

Notice that we do not say that b has to be positive. Thus, we have that for any integer a, that $a|0$. This follows from the fact that $a \times 0 = 0$ for any integer a. There is also no reason to restrict our attention to positive numbers. Negative numbers can divide one another just as well. We can also say things like $-5|20$, as deduced from the fact that $-4 \times -5 = 20$.

While it is true that you can not unscramble an egg (not without a large expenditure of energy, anyway), multiplication can be undone. Just as scientists are fond of breaking down compounds into their component elements and elements into their component atoms, sometimes we like to break down large numbers into the smaller numbers out of which they are made. Thus we might start with the number 100 and notice that $100 = 25 \times 4 = 5^2 \times 2^2$. Here the process ends, since the numbers two and five can not be further broken down.

Indeed, it is easy to see that no matter what number we start with, there must come a time when we reach numbers that can not be broken down any farther. This is so because the divisor of any integer must be smaller (in absolute value, if we are dealing with a negative number) than the integer

itself. Since zero is the smallest absolute value there is, we see that we can not continue breaking down an integer into smaller pieces indefinitely.

From now on let us assume that we are dealing explicitly with positive integers. The numbers residing at the end of such a chain of factorizations will have the property that their only divisors will be one and themselves (for if they had other divisors, we could continue breaking them down). Such integers are referred to as *prime* numbers. The primes can be viewed as the atoms out of which integers are made. We declare by fiat that the number one is not prime, even though it does satisfy the definition we gave a moment ago. We do not make large numbers by starting with smaller numbers and multiplying by one.

We already know that any number can be factored into primes. But is it possible that this factorization is not unique? Earlier we started with 100, factored it into 25×4 and then into $5^2 \times 2^2$. But we could also have started by writing

$$100 = 50 \times 2 = 25 \times 2 \times 2 = 5^2 \times 2^2$$

or

$$100 = 10 \times 10 = 5 \times 2 \times 5 \times 2 = 5^2 \times 2^2.$$

So in this case it seems that no matter how we begin our factorization, we always end up with the same primes at the end. But is this always true?

Indeed it is. To prove this, we first need to introduce some other notions.

If a and b are two integers then we could list all the numbers that divide a and all the numbers that divide b. Since the number one divides every integer, it will appear on both lists. It is possible that some other numbers will also appear on both lists as well. The largest number appearing on both lists is known as the *greatest common divisor*, or GCD, of a and b, written (a, b). It is not lost on me that this is the same as the notation for the ordered pair (a, b), but it will be clear from the context which meaning we have in mind.

If $(a, b) = 1$, meaning that the largest number dividing both a and b is one, then we say that a and b are relatively prime. Alternatively, the fraction $\frac{a}{b}$ is in lowest terms. It is an amusing fact that if a and b are relatively prime, then we can find integers x and y (at least one of which is negative) such that

$$ax + by = 1.$$

Proving this requires a gadget called *the Euclidean algorithm*. Since introducing that here would be far more trouble than its worth, I will ask you to

accept this one on faith.

Having accepted that statement, however, we can now prove the following:

Lemma 2. *Let a, b and c be integers such that $a|bc$ and $(a,b) = 1$. Then $a|c$.*

Proof. Suppose $a|bc$ and $(a,b) = 1$. Then there are integers x and y such that

$$ax + by = 1.$$

From this it follows that

$$acx + bcy = c.$$

Clearly $a|acx$. By assumption, we have $a|bcy$ as well. Since the sum of two multiples of a is again a multiple of a, we see that $a|acx + bcy$ as well. But this says $a|c$, as desired. □

An interesting corollary of this is that if p is prime, $p|ab$ and $p \not| a$, then $p|b$. This follows from the observation that if $p \not| a$ then $(a,p) = 1$. Now we can apply our lemma. Of course, there is nothing special about taking the product of two numbers. The same result holds for products of three or more integers as well.

This says that if a prime number p divides the product of two numbers, then it had to divide one of the two numbers to begin with. To see the significance of this, consider what happens if we try this without a prime number. For example, we observe that $6|(8)(3)$ and $6 \not| 8$, but also $6 \not| 3$. Of course, six is not prime. We see that it is essential to our lemma that p be a prime number.

So what went wrong? Well, six is just a fancy of writing two times three. Meanwhile, eight is two times four. Speaking informally, we see that the ingredients for making up a six were split up between the eight and the three. You see, non prime numbers can be broken up into smaller pieces. These pieces can then be divided between the numbers a and b. In this way a non-prime number might divide the product ab without dividing either piece individually. This is precisely what you can not do with primes. Prime numbers can not be broken down in this way. Hence, the lemma.

Armed with this lemma, we can now smite the problem of proving the uniqueness of a prime factorization. For suppose that some integer x has two different prime factorizations. We will write:

$$p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = q_1^{b_1} q_2^{b_2} \cdots q_\ell^{b_\ell},$$

where the p_i's and the q_i's are prime numbers. Notice that at the moment we are not even assuming that $k = \ell$.

We now observe that p_1 divides the left-hand side. It therefore divides the right-hand side as well. By using the lemma we conclude that $p_1|q_i$ for some i. But since q_i is prime, this is possible only if $p_1 = q_i$. We can assume, without loss of generality, that $p_1 = q_1$. If we now divide both sides by p_1 we get

$$p_2^{a_2} \cdots p_k^{a_k} = q_2^{b_2} \cdots q_\ell^{b_\ell}.$$

We could now repeat the process to discover that $p_2 = q_2$ and so on. We continue in this manner until all of the p_i's are exhausted. At this point we will find that we have exhausted the q_i's as well. For if this does not happen, we would have a product of prime numbers equaling one, which is not possible.

5.2 Least Common Multiple

Before leaving this topic behind, there is one more item that ought to be mentioned. Just as we can start with any positive integer and break it down into its prime factors, we can also start with any integer and consider its multiples. Thus, the number 24 breaks down into $2^3 \times 3$, and its multiples build up through 48, 72, 96 and so on. If we take any two integers and begin listing their multiples, we will eventually find that some integer appears on both lists. For example, if our two integers are x and y then the number xy will appear twice. It follows that there must be some smallest number that appears on both lists, and this number is called the *least common multiple* or LCM of x and y. This is denoted by $[x, y]$.

We find that the LCM of 24 and 36 is 72 and that the LCM of 17 and 13 is 221 which happens to be 17×13.

Both the GCD and the LCM of two integers can be characterized by their prime factorizations. Notice that if

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

denotes an arbitrary integer, then the prime factorization of any divisor d of n must take the form

$$d = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$$

where $0 \leq b_i \leq a_i$ for all i. In other words, the prime factorization of any divisor of n can use only the primes making up n, taken to an exponent no greater than a_i.

Now suppose that x and y are two arbitrary positive integers. If d is a common divisor of x and y, then all of the primes appearing in the factorization of d must also appear in the factorizations of x and y. The greatest common divisor of x and y will be obtained by choosing the exponent of these primes to be as large as possible.

For example: let $x = 72 = 2^3 \times 3^2$ and $y = 405 = 3^4 \times 5$. Then the GCD of x and y is the number $2^0 \times 3^3 \times 5^0$ which is 27. Since the primes 2 and 5 appear in the factorizations of only one of the two numbers, they can not appear in the factorization of any common divisor of x and y.

As a more extravagant example, let

$$x = 23^7 \times 43^8 \times 101^{20} \times 103^{13}$$

and let

$$y = 13^{17} \times 23^{12} \times 29^{48} \times 97^{25} \times 103^{10}.$$

Then the GCD of x and y is

$$d = 13^0 \times 23^7 \times 29^0 \times 43^0 \times 97^0 \times 101^0 \times 103^{10} = 23^7 \times 103^{10}.$$

In general, let x and y be two integers and let $p_1, \cdots, p_k$ be a complete listing of all the primes appearing in the factorizations of either of the two numbers. Let $x = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ and $y = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$, where we leave open the possibility that some of the exponents might be equal to zero. Then

$$(x, y) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_k^{\min(a_k,b_k)}.$$

What about the LCM? Well, if m is a common multiple of two numbers x and y, then the prime factorizations of x and y must be embedded in the prime factorization of m. Thus, if $x = 72$ and $y = 405$, then the LCM is $m = 2^3 \times 3^4 \times 5$. In the more extravagant example above we find that

$$[x, y] = 13^{17} \times 23^{12} \times 29^{48} \times 43^8 \times 97^{25} \times 101^{20} \times 103^{13}.$$

In general, if x and y have the factorizations described above, then

$$[x, y] = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_k^{\max(a_k,b_k)}.$$

An amusing consequence of this is the following observation:

$$\begin{aligned}(x,y)[x,y] &= \left(p_1^{\min(a_1,b_1)}\cdots p_k^{\min(a_k,b_k)}\right)\left(p_1^{\max(a_1,b_1)}\cdots p_k^{\max(a_k,b_k)}\right)\\ &= p_1^{\min(a_1,b_1)+\max(a_1,b_1)}\cdots p_k^{\min(a_k,b_k)+\max(a_k,b_k)}\\ &= p_1^{a_1+b_1}\cdots p_k^{a_k+b_k}\\ &= xy.\end{aligned}$$

We have thus proven the general result:

Theorem 18. *If x and y are positive integers, then $xy = (x,y)[x,y]$.*

5.3 Congruences

Let us suppose that today is Monday and that you want to know the day of the week twenty-three days from now. One way to approach this problem is to remember that every seventh day is Monday. It follows that twenty-one days from now will be Monday again. So twenty-three days will put us at Wednesday.

Similarly, if today is Monday then what day of the week will it be 253 days from now? To solve this we need only realize that 252 is a multiple of seven, and therefore will be a Monday. Consequently, 253 days from now will be a Tuesday.

As one final example, suppose that it is currently noon and you want to know the time $23,999,999$ hours from now. Since this is just one hour less than $24,000,000$, which is a multiple of 24, we deduce that $23,999,999$ hours from now will be $11:00$ in the morning.

In the first two examples, we did not care about the actual number of days, we only cared about the remainder this number left upon division by seven. In the third example, it was not the raw number of hours that mattered, but only the remainder this number left when divided by 24.

Let us fix a positive integer m. Let x and y be arbitrary positive integers. We say that "x is *congruent* to y *modulo* m" if x and y leave the same remainder when divided by m. Alternatively, we can say that $x - y$ is a multiple of m. In this case we write $x \equiv y \pmod{m}$.

Thus, we might say that $42 \equiv 26 \pmod{8}$ and $15 \equiv 75 \pmod{5}$ and $15 \equiv 53 \pmod{1}3$ but $5 \not\equiv 17 \pmod{6}$.

When working modulo m, we see that any integer x must be equivalent to one of the numbers 0 through m. This follows from the fact that there are only m possible remainders that you can leave upon division by m. The number r lying between 0 and m that is congruent to x is referred to as the *least residue of x mod m.*

It is a curious fact that if $x_1 \equiv y_1 \pmod{m}$ and $x_2 \equiv y_2 \pmod{m}$ then $x_1 + x_2 \equiv y_1 + y_2 \pmod{m}$. This follows from the observation that, from the first statement we have $x_1 - y_1$ is a multiple of m while from the second statement we have that $x_2 - y_2$ is a multiple of m. From this it follows that $x_1 - y_1 + x_2 - y_2$ is a multiple of m, as desired.

Equally curious is the fact that $x_1 x_2 \equiv y_1 y_2 \pmod{m}$. To prove this, observe that since $x_1 - y_1$ and $x_2 - y_2$ are multiples of m, we must also have that $y_2(x_1 - y_1)$ and $x_1(x_2 - y_2)$ are multiples of m. But this implies that

$$y_2(x_1 - y_1) + x_1(x_2 - y_2) = x_1 x_2 - y_1 y_2$$

is also a multiple of m.

To be concrete, let us use the number 7 for m. Then we have shown, for example, that if $x \equiv 4 \pmod{7}$ and $y \equiv 5 \pmod{7}$ then $x+y \equiv 4+5 \equiv 9 \equiv 2 \pmod{7}$ and $xy \equiv 4(5) \equiv 20 \equiv 6 \pmod{7}$.

To put this more extravagantly, let us imagine partitioning the integers into seven sets, each one representing a possible remainder that you might leave when divided by 7. Thus, one of the sets will contain all of the multiples of seven, another will contain all the numbers leaving a remainder of one when divided by seven, and so forth until we reach the last set which contains all the numbers leaving a remainder of six when divided by seven. Then what we have done is to define a method for adding and multiplying these sets.

For example, let $\overline{2}$ denote the set of all numbers leaving a remainder of 2 when divided by seven and let $\overline{3}$ denoted the set of all numbers leaving a remainder of 3 when divided by seven. Then to determine $\overline{2} \times \overline{3}$ we begin by choosing one representative out of each of these sets. We observe, for example, that $9 \in \overline{2}$ and $10 \in \overline{3}$. We see that $9 + 10 = 19$ and that $19 \in \overline{5}$ while $9 \times 10 = 90 \in \overline{6}$. Therefore we can say that

$$\overline{2} + \overline{3} = \overline{5} \text{ and } \overline{2} \times \overline{3} = \overline{6}.$$

Put yet another way, the remainder of a sum or a product is the sum or product of the remainders.

5.4 Divisibility Rules

As an application of our musings about congruences, let us ponder the divisibility rules you learned in your mathematical babyhood.

Everyone knows that to determine if a number is a multiple of two you need only consider the final digit. If that digit is even, then so is the whole number, and if that digit is odd then the number is odd. Everyone also knows that a number is a multiple of five if and only if its final digit is a zero or five and that a number is a multiple of ten if and only if its final digit is zero.

Less well-known is the fact that a number is a multiple of three only if its digits add up to a multiple of three. This trick works for nine as well, but it does not work for four. To determine if a number is a multiple of four, you look at its last two digits. If those digits from a multiple of four, then the whole number is a multiple of four. Thus, $135,863,324$ is clearly a multiple of four because its last two digits, 24, form a multiple of four.

When you learn these techniques in elementary school they are usually presented as arbitrary rules that you are expected to memorize. Now we are in a position to see why they are true.

The key to proving all of these rules lies in the fact that any integer can be written in expanded notation. By this I mean that you can, for example, write

$$3847 = (3 \times 10^3) + (8 \times 10^2) + (4 \times 10) + 7$$

or

$$26,234 = (2 \times 10^4) + (6 \times 10^3) + (2 \times 10^2) + (3 \times 10) + 4$$

or

$$31 = (3 \times 10) + 1.$$

Now let us suppose that we wish to determine whether a number is divisible by two. In other words, we seek the remainder our number leaves when divided by two.

To be concrete, let us use the number $31 = (3 \times 10) + 1$. Using what we learned in the last section, we find that we can figure out the remainders of (3×10) and 1 when divided by two, and then simply add these together. Further, to determine the remainder left by 3×10 when divided by 2, we can work with the three and the ten individually. Thus, we see that 10 is an even number, and therefore leaves a remainder of zero when divided by two. It follows that ten times anything will still be even. So 3×10 leaves a remainder of zero.

In general, we notice that every integer can be written as the sum of a multiple of ten plus its final digit. For example, $245 = 240 + 5$. We know that any multiple of ten is even because ten is itself even.

This also shows why any multiple of ten must end in 0. Since every number can be written as the sum of a multiple of ten with its final digit, we see that the only way a number can be a multiple of ten is for its final digit to be a multiple of ten. The only digit satisfying this requirement is 0. Since the only digits that are multiples of five are 0 and 5, we obtain that divisibility rule as well.

What about divisibility by four? The key realization here is that every number if the sum of a multiple of one hundred plus its final two digits. Any multiple of one hundred is clearly a multiple of four. It follows that we need only consider the number formed from the last two digits. For example, $3847 = 3800 + 47$. Since 3800 is a multiple of four, we need only worry about the 47. We notice that, actually, 47 leaves a remainder of 3 when divided by four. We conclude that 3847 leaves a remainder of three when divided by four.

Another way of expressing this is to observe that every power of ten beyond ten itself is a multiple of four.

A similar statement could be made concerning eight. Evert power of ten beyond 100, namely $1,000$, $10,000$ and so forth, is a multiple of eight. Since any number can be written as the sum of a multiple of one thousand plus its final three digits, we conclude that number is a multiple of eight only when its last three digits are.

Which brings us to the vexing case of three and nine. It is a sad fact of life that no powers of ten are multiples of three or nine. However, we do have the next best thing. Observe that any number that is one less than a non-trivial power of ten is always composed of a series of nines. For example, one less than $10,000$ is the number $9,999$. Such a number is clearly a multiple of both three and nine. It follows that every power of ten is one more than a multiple of nine, and consequently one more than a multiple of three as well.

To illustrate the next step, we will assume that we have a four digit number $N = d_4d_3d_2d_1$. I emphasize here that the d_i's are to be thought of as the digits making up the number. We are not multiplying four digits together. I also emphasize that there is nothing special about four digit numbers. That is an assumption we are making just to simplify the reasoning. The same argument will work for numbers of any size.

We begin by writing N in expanded notation:

$$N = 1000d_4 + 100d_3 + 10d_2 + d_1.$$

Our goal is to determine the remainder this number leaves when divided by three. Our reasoning in the previous section reveals that we can do this by examining the remainders left by $1000d_4$, $100d_3$, $10d_2$ and d_1 individually, and then adding together the results.

First we consider $1000d_4$. By again invoking the results of the previous section we know that we can consider the 1000 and the d_4 separately, and multiply their remainders together. The number 1000 leaves a remainder of one when divided by four. From this it follows that the numbers $1000d_4$ and d_4 leave the same remainder upon division by three.

Exactly the same argument shows that $100d_3$ leaves the same remainder as d_3 when divided by three, and likewise for d_2.

The conclusion we draw from all this is that the remainder that

$$1000d_4 + 100d_3 + 10d_2 + d_1$$

leaves when divided by three is the same as the remainder left by

$$d_4 + d_3 + d_2 + d_1$$

which is the sum of the digits of N.

This technique also works for nine, since every power of ten is one more than a multiple of nine. But it does not work for, say, seven, because it is not the case that every power of ten leaves a remainder of one when divided by seven.

For that matter, the remainders left when powers of ten are divided by seven do not reveal any nice pattern. That is why there is no divisibility rule for seven.