Chapter 5

Using the Integers

In spite of their being a rather restricted class of numbers, the integers have a lot of interesting properties and uses. Math which involves the properties of integers is called **number theory**.

5.1 Divisibility

An integer n is **divisible** by an integer m if n is an integral multiple of m. For example, 15 is divisible by 3 because $15 = 5 \cdot 3$. The numbers which divide a given integer are called its **divisors**; for example, the divisors of 12 are 1, 2, 3, 4, 6, and 12 (which divides itself because $12 = 12 \cdot 1$).

EXERCISE 5-1 Write down all the divisors of 20.

Primes are integers which have no divisors except themselves and 1. For example, 7 is a prime, but 8 is not because 2 and 4 divide 8. Numbers like 8 which do have divisors other than 1 and themselves are called **composite**.

WARNING: 1 is NOT considered prime! Unfortunately, it is not composite either. (The reasons for this are too complicated to get into now.) The primes less than 10 are thus 2, 3, 5, and 7.

EXERCISE 5-2 Write down all primes between 11 and 20 inclusive.

EXERCISE 5-3 How many even primes are there?

The notation for one number dividing another is to put a vertical line between them, as in $13|26$ and $12|24$. To indicate that the first number does not divide the second, we put a slash through the line: $11 \not| 23$.

5.2 Number Bases

We can write the integer 7965841 as

$$7000000 + 900000 + 60000 + 5000 + 800 + 40 + 1.$$

That we can write it this way is a consequence of the fact that our usual number system is **base 10**, meaning we have 10 digits. Each digit represents a multiple of a power of 10, based on its position. To make this clearer we could write

$$7 \times 10^6 + 9 \times 10^5 + 6 \times 10^4 + 5 \times 10^3 + 8 \times 10^2 + 4 \times 10^1 + 1 \times 10^0.$$

Why do we count the way we do, following the number 9 with a new number consisting of a 1 and a 0? Having used 10 digits (0 through 9) to count to 9, we make a new "tens place," and assume that the digit in that position is the number of tens. For example, 57 is 5 tens and 7 ones. This saves us from needing a new digit for each number; we can stick to our original ten digits. When we get up to 99, we need to add another place, making the next position represent the number of hundreds.

Humans use 10 digits because we have ten fingers. However, what if we were cartoon characters, with only 8 fingers? Then we might only use the eight digits 0, 1, ..., 7. To go higher than 7, we would create an "eights place," so that 25 in our new number system would represent two 8's and five 1's, or $2(8)+5 = 21$ in the base ten system. Higher positions would correspond to higher powers of 8; for example, 6543 means $6 \times 8^3 + 5 \times 8^2 + 4 \times 8 + 3$. To get rid of the confusion of going back and forth between the two bases, we use the notation that 47_{10} means the base 10 number 47 and 47_8 means the base 8 number 47. (What is this in base 10?) This notation carries over into other bases as well.

EXAMPLE 5-1 What is the base 7 number 3456_7 in base 10?

Solution: All we have to do is write

$$3 \times 7^3 + 4 \times 7^2 + 5 \times 7^1 + 6 \times 7^0 = 3(343) + 4(49) + 5(7) + 6(1) = \mathbf{1266}.$$

EXAMPLE 5-2 Write the base 10 number 216 in base 4.

Solution: The first few powers of 4 are 1, 4, 16, 64, 256, ... Clearly we can't use 256 or any greater power. The highest power which is less than 216 is $64 = 4^3$. The multiples of 64 are 64, 128, and 192; since $192 = 64 \times 3$ is still less than 216, the first digit is 3. Why don't we just use 2 64's? If so we would need more than 3 16's, but we are only allowed 3 nonzero digits to represent the number of 16's. Try it and see! To find the second digit, we look at what is left once we have taken out three 64's, or $216 - 192 = 24$.

In general, to find how many times one number goes into another, we can divide the first by the second and throw out the remainder. Doing this with 24 and 16, the quotient is 1.5, so only one 16 is needed (two 16's are too many), and the second digit is 1. We subtract this 16 from what is left, to get $24 - 16 = 8$. Dividing this by $4^1 = 4$, the quotient is 2, so the third digit is 2. Subtracting $8 - 2 \cdot 4$, we get zero, so the remaining digit is zero since we don't need any 1's. The number in base 4 is $\mathbf{3120_4}$.

EXERCISE 5-4 Find the base 10 representations of 47_8, 47_9, and 47_{16}.

EXERCISE 5-5 Find the base 8, 9, and 16 representations of 47_{10}.

The presence of base 16 in the previous exercises raises a new question: what if we want to use a base greater than 10? We will need more digits than the usual 10, so all we do is use some other symbols. The most common such case is base 16, or **hexadecimal** (six-plus-ten-imal). Here we use the digits

$$0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ A,\ B,\ C,\ D,\ E,\ F.$$

Thus $A_{16} = 10_{10}$ and $F_{16} = 15_{10}$. If we had a high enough base we might have to start using smiley faces and triangles for digits, but there would be little use for such a system.

EXERCISE 5-6 Find the base 10 equivalents of BEE_{16}, DEF_{16}, and $A1_{16}$.

At the opposite extreme from all these digits is the lowly base 2, or **binary**. Here the only two digits are 0 and 1, and counting looks like 1, 10, 11, 100, 101, 110, ...

EXERCISE 5-7 How do you multiply a number by 2 in base 2?

EXERCISE 5-8 Do some conversions into and out of binary.

EXAMPLE 5-3 Perform the addition $1001110_2 + 11001101_2$ without converting the two numbers to decimal. Check your answer by converting to decimal, adding, and converting back.

Solution: We can do the addition just like ordinary base 10 addition, writing the numbers one above the other like so:

$$\begin{array}{cccccccc} & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ \hline \end{array}$$

If two 0's are in a column, a zero goes in the result in the same column. If a 1 and a 0 are in a column, a 1 goes below. If two 1's are together, the sum is 2, which in binary is 10_2. Thus we must carry the 1, and put a 0 below. The 'carrying' process works in base 2 just like in base 10. (Compare this process to adding 56 and 65 in base 10.) This carried 1 will add to the numbers in the next column, making 1 if both are 0, 2 (or 10_2) with a 1 and a 0, and 3 (or 11_2) with two 1's. For the latter two we will have to carry another 1, and so on. Using these rules we can fill in the digits of the result from right to left, as usual:

$$\begin{array}{cccccccccc} 1 & 1 & & & & 1 & 1 & & & \\ & & 1 & 0 & 0 & 1 & 1 & 1 & 0 & \\ & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & \\ \hline 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & \end{array}$$

We've placed the carried digits above the columns they're carried to. The result is $100011011_2 = 256 + 16 + 8 + 2 + 1 = 283_{10}$. To confirm this we convert the original numbers to decimal, getting $1001110_2 = 64 + 8 + 4 + 2 = 78_{10}$ and $11001101_2 = 128 + 64 + 8 + 4 + 1 = 205_{10}$, and note that $205_{10} + 78_{10} = 283_{10}$, as desired.

We have seen that the operation of carrying works in binary. This procedure works in any base. Say we are adding the base 7 numbers 235_7 and 114_7. When we add the two rightmost digits we get $9 = 12_7$, so we place a 2 below the line and carry the 1.

5.3 The Last Digit

No matter what number base we are using, often the most important digit of a number is the last digit. Why should the last digit be so important? There is a very simple reason: if we want to know the last digit of the sum or product of two numbers, all we have to do is find the sum or product of their last digits and take the last digit of that result.

EXERCISE 5-9 Convince yourself that the previous statement is true. Find the last digits of $34 \cdot 17$ and $34 + 17$, first by actually doing the multiplication and addition, then by taking the last digits and just multiplying or adding those. Explain why this works.

The method of the last digit works in any number base and can be used to prove some very useful facts.

EXERCISE 5-10 In base 10, what digits can the last digit of the square of an integer not be?

EXAMPLE 5-4 Find the units digit of $7^{42} + 42^7$.

Solution: To find the last digit of $7^{42} + 42^7$, we find the last digit of each of the two quantities in the sum. To find the last digit of 7^{42}, we break it up into a product of 7's. Since $7^2 = 49$, 7^2 ends in 9. Since $7^4 = 7^2 \cdot 7^2$, it ends in the same number as $9 \cdot 9$ ends in, or 1. Now we write $7^{42} = (7^4)^{10} \cdot 7^2$. Since 7^4 ends in 1, the last digit of $(7^4)^{10}$ is the same as the last digit of the product of ten 1's, or 1. Finally, since $(7^4)^{10}$ ends in 1 and 7^2 ends in 9, 7^{42} ends in $1 \cdot 9 = 9$.

In finding the last digit of 42^7, the tens digit is irrelevant because it does not contribute to the units digit of the product. Hence we are only concerned with 2^7. Since this is 128, the last digit of 42^7 is 8. (Make sure you see why the last digit of 42^7 is the same as that of 2^7.) Completing our problem, $7^{42} + 42^7$ ends in the same digit as $9 + 8$, or **7.**

5.4 Modular Arithmetic

Imagine we decide to do all arithmetic in base 5. Doing arithmetic in different number bases is not always easy; for example, you don't want to memorize a multiplication table for base 16. ($B \cdot C = 84$?!) So just to make it easier on ourselves, we will consider only the last digits. All numbers which have the same last digit in base 5 will be considered equal:

$$2_5 = 12_5 = 22_5 = 32_5 = \cdots$$

In base 10, this looks like

$$2 = 7 = 12 = 17 = \cdots$$

The usual way to show that we are using this system is to replace the = with a $\equiv$, and also append the suffix (mod 5). We thus write, for example, $12 \equiv 7 \pmod 5$. We say that **12 is congruent to 7 mod 5**.

Another way to look at mods is that 2, 7, 12, 17, etc. all have the same remainder (2) when divided by 5. This method of viewing modular arithmetic makes actual computation much easier. It is often

useful to find the smallest nonnegative integer which is congruent to x mod y. (For example, the smallest integer congruent to 12 mod 5 is 2.) When we perform this task, we say that we 'mod out' the 12. Now you see how our second way of viewing mods is useful. To mod out 7631 in mod 7, we can either find 7631 in base 7 and look at the last digit, or we can divide by 7 and look at the remainder.

In this discussion of remainders, we have used mods to denote the amount more than a multiple of 5 a given number is. For example, 2, 7, 12, 17, etc. are all exactly 2 more than a multiple of 5. In the same way we can define negative mods as the amount less than a multiple of 5 a number is. Since 2, 7, 12, 17, etc. are all 3 less than the nearest multiple of 5, they are all congruent to -3 mod 5. Extending this reasoning, we can write in mod 5:

$$\cdots \equiv -13 \equiv -8 \equiv -3 \equiv 2 \equiv 7 \equiv 12 \cdots$$

Note that each term is five away from the one before it and after it. Think about why this is true.

EXAMPLE 5-5 Why does the remainder method described above work?

Solution: Consider 7631 in base 7. It is 31151_7, or

$$3 \cdot 7^4 + 1 \cdot 7^3 + 1 \cdot 7^2 + 5 \cdot 7 + 1.$$

When we divide this expression by seven, the seven evenly divides the first 4 terms of the sum and leaves the last term as the remainder, i.e. $7631/7 = 3 \cdot 7^3 + 1 \cdot 7^2 + 1 \cdot 7 + 5$, with a remainder of 1. Hence we see that the last digit of 7631 written in base 7 is the same as the remainder we have upon dividing 7631 by 7. This is why the remainder method works.

EXERCISE 5-11 Write down some numbers which are congruent to 3 mod 5.

EXERCISE 5-12 What is the largest integer less than 100 which is congruent to 3 mod 5?

EXAMPLE 5-6 How many positive integers less than 100 are congruent to 3 mod 5?

Solution: The smallest is obviously 3. In the previous exercise, you should have found that the largest is 98. How many are there in between? We have $3 = 0(5) + 3$ and $98 = 19(5) + 3$, and the other numbers congruent to 3 mod 5 will be $1(5) + 3$, $2(5) + 3$, and so on. The number by which 5 is multiplied can be $0, 1, 2, \ldots, 19$, so there are **20** possibilities.

EXERCISE 5-13 How many integers are there between 50 and 250 inclusive which are congruent to 1 mod 7?

EXERCISE 5-14 Which numbers are congruent to 0 mod 5?

Once the principle of congruence is understood, we can move on to doing actual arithmetic with it. One thing which we can do with a congruence like

$$12 \equiv 7 \pmod 5$$

is add the same thing to both sides:

$$12 + 3 \equiv 7 + 3 \pmod 5.$$

We can do this because if the last digits in base 5 are the same before the addition, they will be the same after the addition. Clearly the same will be true for subtraction.

How about for multiplication? Again, the same should hold. If the last digits are the same before the multiplication, they will be the same after.

Not only can we multiply or add the same quantities to both sides, but if x and y have the same last digit in base 5, then we can add x to one side and y to the other in mod 5. For example, since 8 and 13 have the same last digit in base 5,

$$12 + 13 \equiv 7 + 8 \pmod 5.$$

Applying this concept to multiplication, since 12 and 7 are congruent mod 5, we can multiply one side by 12 and the other by 7, yielding

$$12^2 \equiv 7^2 \pmod 5.$$

In this manner, we can raise the two sides to any positive integral power!

WARNING: Division is a much more complicated matter. For instance, clearly $5 \equiv 10 \pmod 5$, but if we divide both sides by 5, we have $1 \equiv 2 \pmod 5$, an obviously false relation. There is something wrong here, and that something will be investigated in the next volume. Just remember that division doesn't generally work in modular arithmetic.

In finding the last digit of a sum or product of two numbers, we don't need to do the entire sum or product, just the sum or product of the last digits of the two numbers. In mods, this is reflected by the fact that we can "mod out" before or after doing operations; the order doesn't matter. By this we mean that we can mod out the factors of a product and then multiply the results rather than having to mod out the product of the numbers. For example, since $9899 \equiv 4 \pmod 5$ and $7677 \equiv 2 \pmod 5$, we can say $9899 \cdot 7677 \equiv 4 \cdot 2 \equiv 8 \equiv 3 \pmod 5$ rather than first multiplying 9899 and 7677 and modding out the product. Make sure you follow this; it is a very important technique. Try to use it to show that $9453 \cdot 6824 \equiv 6782 \cdot 5675341 \equiv 2 \pmod 5$.

Let's summarize what we can do with congruences. If $a \equiv b \pmod m$ and $p \equiv q \pmod m$, then for all positive integers c, we have:

1. $a + c \equiv b + c \pmod m$
2. $a - c \equiv b - c \pmod m$
3. $ac \equiv bc \pmod m$
4. $a^c \equiv b^c \pmod m$
5. $(a + p) \equiv (b + q) \pmod m$
6. $ap \equiv bq \pmod m$

You may need to chew on those last two a bit, though they are among the most useful. They just restate the fact that we can mod out before or after we add or multiply.

EXAMPLE 5-7 If we are given that $a \equiv 0 \pmod{b}$, then the remainder when a is divided by b is 0. Thus we can conclude that a is a multiple of b.

EXERCISE 5-15 Find the smallest positive integer which 123 is congruent to mod 4. Find the smallest positive integer that 321 is congruent to mod 7.

EXERCISE 5-16 Show that the square of any integer is congruent to either 0, 1, or 4 mod 8.

5.5 Divisibility Tricks

Even at this early stage in understanding divisibility, we can find some tricks to tell if one number divides another. We start with the obvious example: a number is divisible by 10 if and only if its last digit is 0. This seems trivial, but then so will the rest of the rules in this section when you've used them a few times.

We start with the basic concept that a number, x, is divisible by another number, y if and only if $x \equiv 0 \pmod{y}$. This just means that when we divide x by y, the remainder is zero.

First we examine divisibility by 2. A number is divisible by 2 if and only if it is congruent to 0 mod 2. We can write the number, say 7965841, as the sum of its last digit and the rest, as in $7965841 = 1 + 7965840$. Thus we can write $7965841 \equiv 1 + 7965840 \pmod{2}$. The second part ends with a zero, so is divisible by 10, or $7965840 = 10(\text{something})$. But $2|10$, so this means $7965840 = 2(\text{something else})$, so that 2 divides 7965840, and $7965840 \equiv 0 \pmod{2}$. Substituting this in above, we find that $7965841 \equiv 1 \pmod{2}$, or a number is congruent to its last digit mod 2. So to test for divisibility by 2, we just test the last digit, which must be 2, 4, 6, 8, or 0 if the number is to be divisible by 2. We went through this very long method of showing that $2|7965840$ to give a hint as to how we test for divisibility of other numbers.

For example, consider 4. A multiple of 10 is not necessarily a multiple of 4, but a multiple of 100 is. We therefore note that

$$45376 \equiv (45300 + 76) \pmod{4} \equiv ((453 \cdot 100) + 76) \pmod{4}.$$

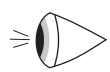
Since $100 \equiv 0 \pmod{4}$, we have $453 \cdot 100 \equiv 453 \cdot 0 \pmod{4}$, which means $453 \cdot 100 \equiv 0 \pmod{4}$, and now we have

$$45376 \equiv ((453 \cdot 100) + 76) \pmod{4} \equiv ((453 \cdot 0) + 4 \cdot 19) \pmod{4} \equiv (0 + 0 \cdot 19) \pmod{4} \equiv 0 \pmod{4}.$$

Notice how useful the fact that $100 \equiv 0 \pmod{4}$ is to showing that 45376 is a multiple of 4.

EXERCISE 5-17 Find a shortcut along the same lines to test for divisibility by 5.

EXERCISE 5-18 How about for 4, 8, and 20?



EXERCISE 5-19 Why is it so easy to test for divisibility by these numbers?