Abstract

This is an introduction to more advanced topics in number theory suitable for an advanced Grade 4 audience. These notes were prepared for the Grand River Chinese School. Each chapter may take two to four hours to deliver entirely, depending on the level of detail.

These notes are intended to be a rough outline of what is taught, and not a rigorous and complete reference. I do not necessarily cover all the material written in these notes in any particular year, and I may occasionally cover material beyond that written in the notes.

Although the notes are intended to be presented to a young audience, they are written for a teacher and not for a student. Many of the terms used will not be familiar to the students, and will need to be explained differently.

Number Theory

Fengyang Wang

April 7, 2016

Contents

Chapter 1

Parity & Divisibility

Number Theory is the study of whole numbers. That means 0, 1, 2, and so on. Number Theory also studies negative whole numbers, such as -1, -2, and so on. Positive and negative whole numbers, and 0, are together called integers.

1.1 Parity

Parity is a property of integers that classifies integers into even integers and odd integers. In this section, we will study the differences between even and odd integers, and also study several important properties. We will approach the problem algebraically.

An even number is a number of the form $2n$, where n is any integer. The expression $2n$ means $2 \times n$; we omit the $\times$ so that it is faster to read and write.

An odd number is a number of the form $2n+1$, where n is any integer. The expression $2n+1$ means $(2 \times n)+1$. We perform the multiplication first because of the order of operations.

1.1.1 Determining Parity

It is easy to determine whether a number is even or odd. Let's start with small examples first. We know $4 = 2 \times 2$, so it's even. We know $7 = 2 \times 3 + 1$, so it's odd. A number is either even or odd, but it's never both. We only need to divide by 2: if it evenly divides, then it's even, and otherwise, it's odd.

Problem 1.1.2 Example

Are each of the following numbers even or odd?

- 10 — [Even] Odd
- 0 — [Even] Odd
- 19 — Even [Odd]
- -1 — Even [Odd]

If the numbers are very big, it is convenient to simply observe the last digit. If the last digit is even, then the whole number is even. If the last digit is odd, then the whole number is odd. Why does this work? We will see very soon.

1.1.3 Sums & Differences

What happens if we add two odd numbers? Two even numbers? Let's find out. Say $2n+1$ and $2m+1$ are two odd numbers. We're using letters here as placeholders; n and m can both take the value of any integer. Then

$$(2n+1)+(2m+1) = 2n+2m+1+1 = 2n+2m+2 = 2(n+m+1)$$

but $n+m+1$ is an integer, and therefore the sum is even.

We can use a very similar strategy to find the sum of two even numbers. This is even easier. Say $2n$ and $2m$ are two even numbers. Then

$$2n+2m = 2(n+m)$$

but $n+m$ is an integer, and therefore the sum is even.

Say $2n$ is an even number, and $2m+1$ is an odd number. Then

$$2n+2m+1 = 2(n+m)+1$$

which is an odd number. So the sum of an even number and an odd number is odd. And because we can rearrange the order of addition, therefore the sum of an odd number and a even number is also odd.

The rules for subtracting are exactly the same. The difference of two odds is even. The difference of two evens is even. The difference of an odd and an even is odd. Feel free to work these out yourself.

Problem 1.1.4 Example

Are each of the following numbers even or odd?

- $100 + 200$ — [Even] Odd
- $1273 + 19023$ — [Even] Odd
- $19082 - 1911$ — Even [Odd]
- $109291 + 8329 + 9107$ — Even [Odd]

1.1.5 Products

We can use a similar technique to develop rules for the product of even and odd numbers. It turns out that the product of two odd numbers is odd. Say $2n+1$ and $2m+1$ are two odd numbers. Observe:

$$\begin{aligned}(2n+1)(2m+1) &= 2n(2m+1)+(2m+1)\\ &= 4nm+2n+2m+1\\ &= 2(2nm+n+m)+1\end{aligned}$$

which is odd.

But the product of an even number with any integer is even. Say $2n$ is an even number, and k is any integer. Then:

$$(2n)k = 2(nk)$$

which is even.

At this point we have enough knowledge to see why our rule for determining parity by looking at the last digit works. In a number written in the place value

system, such as 76103, we can split the number into the ones' digit, the tens' digit, hundreds' digit, and so on. Another way to think about it is, by splitting off the ones' digit,

$$76103 = 3 + 7610 \times 10$$

But we know that $10 = 2 \times 5$ is even, so by the rules covered above, we know that anything mutliplied by 10 remains even. Then if we add it to an odd number, we obtain an odd number, but if we add it to an even number, then we obtain an even number. Therefore, just by looking at the last digit, we can figure out whether a number is odd or even.

1.2 Divisibility

We will begin today's topic with a few definitions.

The symbol | means "divides". If A and B are two numbers, then A divides B when $B \div A$ has no remainder.

A number is a *factor* of another number if it divides that number. For example, 3 is a *factor* of 9 because $3 \mid 9$. A number is a *multiple* of another number if the other number divides it. For example, 9 is a *multiple* of 3. Another word for factor, which we will see later on, is *divisor*.

Observe that 1 is a *factor* of every whole number, and 0 is a *multiple* of every whole number.

1.2.1 Finding Factors

One class of problem that we may be interested in solving is to list the factors for a number. When the number is small, this is easy. For example, listing the factors of 6 is as simple as trying out all smaller (or equal) numbers, and finding that only 1, 2, 3, and 6 divide 6 evenly.

For larger numbers, we may exploit the fact that factors always come in pairs. If $a \mid c$, then there is some number b so that $a \times b = c$. But then we can just flip the order of the multiplication, and we see that $b \times a = c$ and therefore $b \mid c$. Therefore a convenient way to find big factors is to divide the original number by the smaller factors.

1.2.2 Revisiting Parity

Using our new definitions, we see that the topic we covered last class—even and odd numbers—is really just the study of numbers that are and aren't divisible by 2. Even numbers are the multiples of 2, and all even numbers have 2 as a factor. Be careful! Note that odd numbers do not necessarily have 3 as a factor (for example, 5 is not a mutliple of 3), and even numbers might (for example, 6 is a multiple of 3 and is also even.)

1.2.3 Divisibility Rules

Earlier we have already seen rules for divisibility by 2. We have a similar rule for divisibility by 5. The reason that this rule is correct will be discussed later in this unit, but please feel free to think about it. To figure out whether a number is divisible by 5, simply look at the last digit. If it is 0 or 5, then the number is divisible by 5.

For divisibility by 10, the rule is even simpler. A number is divisible by 10 if and only if the last digit is 0. A number is divisible by 100 if the last two digits are 0. (Note that 0 is a bit of a special case, since it only has one digit, but it is still divisible by 100.)

1.2.4 Transitivity

The transitivity principle of divisiblity says that if a, b, and c are integers, and if $a \mid b$ and $b \mid c$, then $a \mid c$. Let's do an example. We know that $3 \mid 12$, and that $12 \mid 36$. Then by transitivity, $3 \mid 36$. Here is a simple exercise that is easily done using transitivity:

Problem 1.2.5 Example

Does 3 divide *every* multiple of 12? [True] False

Solution: Say a is some multiple of 12. By definition, $12 \mid a$. Here we are using a as a placeholder—it can stand for *any* multiple of 12.

Since $12 \div 3 = 4 \,\mathrm{R}\, 0$, we know that $3 \mid 12$. But if $3 \mid 12$ and $12 \mid a$, then by transitivity, $3 \mid a$. Therefore, the statement that 3 divides every multiple of 12 is [true].

1.3 Review

There is a quiz for this unit (Quiz 3: Parity and Divisibility). The allocated length for the quiz is 15 minutes. Three review questions follow. Quiz questions will be very similar in nature.

Problem 1.3.1 Factor Pairs

Complete the factor pairs.

- $6 = 1 \times$ [6]
- $6 = 2 \times$ [3]
- $6 = 3 \times$ [2]
- $6 = 6 \times$ [1]

Problem 1.3.2 Factors and Multiples

Use the word "factor" or "multiple" to complete each blank.

- 1 is a [factor] of every whole number.
- 0 is a [multiple] of every whole number.
- 3 is a [factor] of 9.
- All even numbers are [multiples]s of 2.

Problem 1.3.3 Divisibility

Circle factors of each number. More than one factor may be circled.

- 25 — $\boxed{1}$ 2 $\boxed{5}$ 10 100
- 172 — $\boxed{1}$ $\boxed{2}$ 5 10 100
- 1793 — $\boxed{1}$ 2 5 10 100
- 2000 — $\boxed{1}$ $\boxed{2}$ $\boxed{5}$ $\boxed{10}$ $\boxed{100}$

Chapter 2

Prime Numbers

A *prime number* is a positive integer that has exactly two positive factors: 1 and itself.

2.1 Testing for Primality

We can easily check whether small numbers are prime. First, note 1 is not prime, because it has just one factor. However, 2 is prime, because it has exactly two factors: 1 and itself.

Problem 2.1.1 The First Few Primes

Is each number prime or not prime?

- 2 [Prime] Not Prime
- 3 [Prime] Not Prime
- 4 Prime [Not Prime]
- 5 [Prime] Not Prime
- 6 Prime [Not Prime]
- 7 [Prime] Not Prime
- 8 Prime [Not Prime]
- 9 Prime [Not Prime]
- 10 Prime [Not Prime]

Don't get caught in the trap that every odd number is prime! $9 = 3 \times 3$ is not. Neither are 15, 21, 25, and many others. In fact, as the numbers get bigger and bigger, prime numbers get rarer and rarer. However, do note that there is only one even prime: 2.

2.1.2 For Large Numbers

Checking whether large numbers are prime is much harder to do on paper. However, it is easy to see that some numbers are composite. For example, if a number ends in 0, 2, 4, 5, 6, or 8, then it is probably composite—the only two exceptions are 2 and 5.

As an interesting note, which we will not explore further in this class, there are actually infinitely many prime numbers. That means that no matter how big our prime numbers get, we can always find another bigger prime number.

2.2 Composite Numbers

A *composite* number is a number that can be written as the product of two smaller positive numbers. Thus $4 = 2 \times 2$ is composite. It turns out that every non-prime positive whole number except 1 is composite.

Composite numbers have at least three distinct factors. Usually, they have at least four (such as 6, which has factors 1, 2, 3, and 6), but there is a special category of numbers that have exactly 3. These are the squares of prime numbers. For instance, 4 has factors 1, 2, and 4, and 9 has factors 1, 3 and 9. This happens when the only prime factor of a number is paired with itself.

When numbers get quite large, composite numbers vastly outnumber prime numbers. Many classes of numbers contain only one prime number and infinitely many composite numbers. For instance, among the powers of 2 (2, 4, 8, 16, ...), only 2 is prime.

2.3 The Fundamental Theorem of Arithmetic

One of the most important facts about whole numbers, one that forms the basis for much of number theory, is the Fundamental Theorem of Arithmetic. This theorem is a result that states that every positive whole number can be factored uniquely into primes. What does that mean?

If we have a whole number, say, 70, we see that we can write it as 7×10. Furthermore, $10 = 2 \times 5$. So we can factor $70 = 7 \times 2 \times 5$. Each of these numbers is now prime, and so we cannot factor this further, except by introducing copies of 1, which is pointless.

But what if we had factored it a different way, first writing $70 = 5 \times 14$? Then we notice that $14 = 2 \times 7$, so we can change to $70 = 5 \times 2 \times 7$. The important thing is that this is the same factorization as last time, except in a different order. In fact, no matter, how we factor 70, we will always arrive at the same prime factorization (with possibly a different order).

Problem 2.3.1 Factorize

Find the prime factorization for each number.

- $12 = \boxed{2 \times 2 \times 3}$
- $70 = \boxed{2 \times 5 \times 7}$
- $100 = \boxed{2 \times 2 \times 5 \times 5}$

Problem 2.3.2 Prime Factors

Find one (no need to find all) prime factor for each number.

- 99959386 Factor: $\boxed{2}$
- 521976505 Factor: $\boxed{5}$

As you will see on the homework, it may be difficult to factor very large numbers. In fact, lots of modern cryptography, including the popular RSA encryption scheme, rest on the fact that nobody has yet discovered a fast way to factor large numbers.

2.3.3 Applications to Problem Solving

So far in this unit, we have not done so many applications to problems of the sort typically seen in math contests. However, this does not mean that the Fundamental Theorem of Arithmetic is not useful for contest math. Many questions can be simplified greatly by factorizing numbers into their prime factorizations. It is even useful for mental arithmetic. We will see some examples below.

Problem 2.3.4 Mental Arithmetic

Find, without using a calculator, 1875×48.

Solution: We compute

$$1875 = 5 \times 5 \times 5 \times 5 \times 3$$

and

$$48 = 2 \times 2 \times 2 \times 2 \times 3$$

so

$$\begin{aligned} 1875 \times 48 &= 5 \times 5 \times 5 \times 5 \times 3 \times 2 \times 2 \times 2 \times 2 \times 3 \\ &= 10 \times 10 \times 10 \times 10 \times 3 \times 3 \\ &= \boxed{90000} \end{aligned}$$

Factorizing numbers into primes before multiplying them is a common technique in mental math.

2.3.5 Culture and History

Although the Fundamental Theorem of Arithmetic is known to be true, many people believe that it is not obvious. Why is it that all positive integers can be broken down *uniquely* into prime numbers? In mathematics, claims like the Fundamental Theorem of Arithmetic require proof. That is, we need a convincing argument that it is true for all numbers. The argument should depend only on facts that are known and accepted to be true, or facts that also have proofs. The first known proof for the Fundamental Theorem of Arithmetic was in book VII (7) of Euclid's Elements, propositions 30 and 32. It is beyond the scope of this course.

Chapter 3

Greatest Common Divisor

3.1 Introduction

In this chapter, we will discuss two very important topics that have many applications: the greatest common divisor, and another similar operation, the least common multiple.

3.1.1 Greatest Common Divisor

Given two positive integers, we define their GCD (greatest common divisor) to be the largest positive integer that's a factor for both those numbers. For instance, the factors of 24 are 1, 2, 3, 4, 6, 8, 12, 24, and the factors of 36 are 1, 2, 3, 4, 6, 9, 12, 18, 36. The greatest factor that these have in common is 12. Therefore we denote

$$\gcd(24, 36) = 12$$

Problem 3.1.2 Examples

- $\gcd(10, 20) = \boxed{10}$
- $\gcd(15, 25) = \boxed{5}$
- $\gcd(7, 11) = \boxed{1}$

3.1.3 Least Common Multiple

Similarly, given two positive integers, we define their LCM (least common multiple) to be the smallest positive integer that's a multiple of both those numbers. For instance, the positive multiples of 24 are 24, 48, 72, and so on, and the positive multiples of 36 are 36, 72, 108, and so on. The smallest multiple that these have in common is 72. Therefore we denote

$$\operatorname{lcm}(24, 36) = 72$$

An intriguing connection between the GCD and the LCM is given by the following identity, which we will not justify in this class, but you may see again in the future:

$$\gcd(a, b) \times \operatorname{lcm}(a, b) = a \times b$$

Roughly speaking, this identity says that the product of two numbers is the same as the product of their GCD and their LCM.

3.2 Applications

The GCD and the LCM have many applications across mathematics. One useful application comes from studying fractions. Two fractions are equivalent if, despite the numerator and the denominator possibly differing, they represent the same quantity. For instance, the fraction $\frac{1}{2}$ is equivalent to fractions $\frac{2}{4}$, $\frac{3}{6}$, and so on.

We may *simplify* a fraction by writing it as an equivalent fraction with least possible (positive) denominator. Simplifying fractions makes it easy to determine whether two fractions are equivalent, and also makes fractions easier to work with. There exists a simple algorithm to simplify a fraction. Given $\frac{n}{m}$, compute $d = \gcd(n, m)$, and then $\frac{n \div d}{m \div d}$ is the simplest form.

Problem 3.2.1 Simplify Fraction

Simplify. Note that the fraction may possibly already be in simplest form.

- $\frac{20}{15} = \boxed{\frac{4}{3}}$
- $\frac{24}{36} = \boxed{\frac{2}{3}}$
- $\frac{7}{13} = \boxed{\frac{7}{13}}$

When we add or subtract fractions, it helps often to write the fractions with equal denominator. To select a compatible denominator, we may use the least common multiple. For example, to add $\frac{a}{b} + \frac{c}{d}$, we may compute $\ell = \operatorname{lcm}(b, d)$ and then compute

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &= \frac{a\ell \div b}{\ell} + \frac{c\ell \div d}{\ell} \\ &= \frac{a\ell \div b + c\ell \div d}{\ell} \end{aligned}$$

which then we may simplify with the algorithm described above.

Problem 3.2.2 Adding and Subtracting Fractions

Add or subtract. Then simplify.

- $\frac{1}{2} + \frac{1}{3} = \boxed{\frac{5}{6}}$
- $\frac{3}{4} + \frac{1}{6} = \boxed{\frac{11}{12}}$
- $\frac{23}{36} - \frac{11}{24} = \boxed{\frac{13}{36}}$

3.3 Remainders Review

Before we continue, it is important to have a good grasp of what remainders are, and to introduce some new notation. While this is adequately covered on the homework assignments, a quick recap is provided below.

When we divide 20 by 4, we count how many groups of 4 are needed to make 20. We know that $5 \times 4 = 20$. This means that it takes 5 groups of 4 to make 20. So $20 \div 4 = 5$.

Sometimes the numbers might not work out perfectly. Let's try dividing 20 by 3. If we make 7 groups of 3, the total number would be $7 \times 3 = 21$. But this is too big. If we make 6 groups of 3, the total number would be $6 \times 3 = 18$. But this is too small. So we can make six groups, but we'd then have $20 - 18 = 2$ left over!

We say that when we divide 20 by 3, our *quotient* is 6 because we can make 6 groups of 3 in total. And then we say that our *remainder* is 2 because after making 6 groups of 3, we have 2 left over. We can also write this as $20 \div 3 = 6\,\mathrm{R}\,2$. The "R" stands for "remainder".

Suppose we didn't care what the quotient was; only the remainder is important. Then we can write that as $16 \bmod 5 = 1$. We don't care how many groups we made, but we do care that one was left over after making those groups.

The study of remainders is very useful for several major applications, some of which we will see later this unit. Recalling the patterning unit, we used remainders to compute future terms in repeated sequences. Many of the applications of remainders are based off this application.

3.4 Euclidean Algorithm

An *algorithm* is a "step-by-step procedure for performing a calculation according to well-defined rules" (Wikipedia).

In this lesson we will cover a useful algorithm that allows us to find the greatest common divisor of two large numbers. This algorithm has been known for thousands of years. It was discovered by the Ancient Greeks, and is named after Euclid, one of the most famous mathematicians in history.

This algorithm is based on the fact that the greatest common denominator does not change if the smaller number is subtracted from the larger one. That is, $\gcd(a, b) = \gcd(a, b - a)$ for all positive integers a and b, with $b > a$. Proving this fact is beyond the scope of this course. However, we will look at an example.

Consider $\gcd(8, 12) = 4$. If we subtract 8 from 12, we get $\gcd(8, 4) = 4$. If we subtract now 4 from 8, we get $\gcd(4, 4) = 4$. We notice that the GCD is unchanged despite these subtractions.

To avoid subtracting potentially many times, we can change the repeated subtraction into a remainder operation. Thus we arrive at the most commonly stated version of the Euclidean algorithm:

3.4.1 The Euclidean Algorithm

To find the Greatest Common Divisor of two numbers, a and b:

1. If $a = 0$, then terminate. The greatest common divisor is b.
2. Otherwise, apply the Euclidean Algorithm to find the GCD of $b \bmod a$ and a. That is, $\gcd(a, b) = \gcd(b \bmod a, a)$.

3.4.2 Properties of the Euclidean Algorithm

This algorithm is an example of a recursive algorithm. More specifically, it is a "tail recursive" algorithm. That means that the algorithm either produces a result, or it requires running the algorithm another time on simpler numbers. We may need to run the Euclidean algorithm several times on progressively simpler numbers before finishing the computation.

Although the Euclidean algorithm may take some time to compute by hand, it is very easy for a computer to do. In fact, the algorithm is so efficient that

computers can easily calculate the greatest common divisors of numbers with thousands of digits, in a matter of milliseconds!

3.5 Euclidean Algorithm Examples

Here is a quick example of using the Euclidean algorithm to compute the greatest common divisor of medium-sized numbers:

Problem 3.5.1 GCD of Two Numbers

Compute $\gcd(60, 84) = \boxed{12}$.

Solution:

$$\begin{aligned}\gcd(60, 84) &= \gcd(84 \bmod 60, 60)\\ &= \gcd(24, 60)\\ &= \gcd(60 \bmod 24, 24)\\ &= \gcd(12, 24)\\ &= \gcd(24 \bmod 12, 12)\\ &= \gcd(0, 12)\\ &= 12\end{aligned}$$

We may alternatively seek to find the GCD of multiple (more than two) numbers. This means the largest number that is a divisor of all the numbers we're interested in. We can do this by finding the GCD of the first two, and then finding the GCD of that number and the third, and so on. That is, we use the formula

$$\gcd(a, b, c, d, \dots) = \gcd(\gcd(a, b), c, d, \dots)$$

This computation may require several long and tedious applications of the Euclidean algorithm. Luckily, in practice, when GCDs for large numbers must be computed, computers can typically be used. You will not be required to do problems of this sort on your homework or quizzes.

Problem 3.5.2 GCD of Three Numbers

Compute $\gcd(3636, 3948, 4056) = \boxed{12}$.

Solution:

$$\begin{aligned}
\gcd(3636, 3948, 4056) &= \gcd(\gcd(3636, 3948), 4056) \\
&= \gcd(\gcd(3948 \bmod 3636, 3636), 4056) \\
&= \gcd(\gcd(312, 3636), 4056) \\
&= \gcd(\gcd(3636 \bmod 312, 312), 4056) \\
&= \gcd(\gcd(204, 312), 4056) \\
&= \gcd(\gcd(312 \bmod 204, 204), 4056) \\
&= \gcd(\gcd(108, 204), 4056) \\
&= \gcd(\gcd(204 \bmod 108, 108), 4056) \\
&= \gcd(\gcd(96, 108), 4056) \\
&= \gcd(\gcd(108 \bmod 96, 96), 4056) \\
&= \gcd(\gcd(12, 96), 4056) \\
&= \gcd(\gcd(96 \bmod 12, 12), 4056) \\
&= \gcd(\gcd(0, 12), 4056) \\
&= \gcd(12, 4056) \\
&= \gcd(4056 \bmod 12, 12) \\
&= \gcd(0, 12) \\
&= \boxed{12}
\end{aligned}$$

We may cover a few assorted problems to reinforce your ability to compute the GCD using the Euclidean algorithm. However, in general, this computation is not difficult, but is brainless and long, and I do not recommend you do many of these problems for practice.

Problem 3.5.3 Assorted GCD Problems

Use the Euclidean Algorithm to compute the following:

- $\gcd(12, 28) = \boxed{4}$
- $\gcd(147, 392) = \boxed{49}$
- $\gcd(319, 920) = \boxed{1}$
- $\gcd(2635, 4515) = \boxed{5}$
- $\gcd(12936, 25256) = \boxed{616}$
- $\gcd(399, 1533, 1659, 2016) = \boxed{1}$

Chapter 4

Modular Arithmetic

The final chapter in this unit will be brief, and you will not be quizzed on the material. However, the content of this chapter will certainly be interesting.

In earlier chapters we discussed briefly remainders and some applications. In this chapter, we will develop new powerful techniques to simplify the solution to these problems.

4.1 Generalizing Parity

When we talked about even and odd numbers, we came up with rules about the result of adding, subtracting, and multiplying even and odd numbers. We can come up with similar strategies for divisibility by any number, not just 2. For the purposes of discussing this with greater ease, we will consider 7 as our base.

All positive integers (in fact, all integers, including zero and negative ones) can be categorized into 7 distinct buckets based on their remainder when divided by 7. Let us call these buckets [0], [1], [2], [3], [4], [5], and [6]. In the following table we have categorized the numbers from 0 to 30 into these buckets:

[0]	0	7	14	21	28
[1]	1	8	15	22	29
[2]	2	9	16	23	30
[3]	3	10	17	24	
[4]	4	11	18	25	
[5]	5	12	19	26	
[6]	6	13	20	27	

We can see a few patterns in the above table. When we add 1 to a number, we move to the next bucket. But [6] has no next bucket, so what happens when we add 1 to a number in bucket [6]? We move to bucket [0]! In some sense, these buckets form a sort of cycle. After we reach the last bucket, we loop around and return to the first bucket (Figure 4.1).

This behaviour should make sense when starting at buckets [0] to [5]. But for bucket [6], why is it that we move to bucket [0] by adding one more? We can find the solution using algebra, just like how we did when talking about parity. Any number in bucket [6] looks like $7n + 6$ for some integer n. If we add 1 to this,

$$7n + 6 + 1 = 7n + 7 = 7(n + 1)$$

and we can see that this is a multiple of 7, and so belongs in bucket [0].

We now consider what happens if we add 2 to a number. In which bucket would the new number be in? This is the same as adding 1 twice. So, for

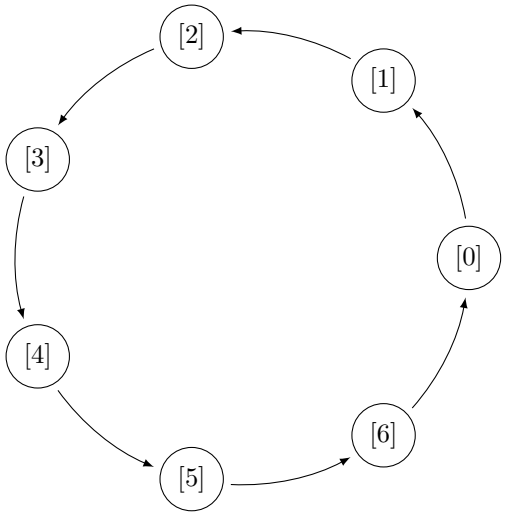

Figure 4.1: When we add 1 to a number in a bucket, we move to the next bucket in this diagram.

example, [0] goes to [2], [4] goes to [6], [5] goes to [0] and [6] goes to [1]. Again, we are just moving around in circles. It is similar to addition on the number line, but instead of going in a line, we are going in a cycle.

The process of addition is moving numbers from one remainder bucket to the next several times. What happens if we add 7? Well, we would have gone one whole cycle around, and so our result should be in the same bucket. And indeed, that is what we would expect, since adding 7 should not change the remainder when dividing by 7.

The same goes for any multiple of 7. If we add 21, we would go around one whole cycle 3 times, and then arrive back where we started. For bigger numbers that are not multiples of 7, we can think of the addition as moving around the whole cycle several times, then moving some extra steps. How many extra steps do we move? Why, the remainder when divided by 7, of course.

To recap, we have devised a system where we can predict the remainder of a sum when divided by 7, knowing just the remainders of the two summands when divided by 7. We simply start at the bucket for the first number and advance a number of buckets in the cycle equal to the remainder of the second number when divided by 7. We introduce the following notation:

$$[1] + [2] = [3]$$

to mean that the sum of a number in bucket [1] and a number in bucket [2] is a number in bucket [3].

We can return to algebra to provide a justification for this behaviour. Say $n \bmod 7 = i$, and $m \bmod 7 = j$. Then let $n = 7k + i$ and $m = 7\ell + j$. We see that

$$\begin{aligned}(n+m) \bmod 7 &= (7k + i + 7\ell + j) \bmod 7 \\ &= (7(k+\ell) + i + j) \bmod 7 \\ &= (i + j) \bmod 7\end{aligned}$$

which is the same as saying that the remainder of the sum of two numbers when divided by 7 is the same as the remainder of the sum of the remainders when divided by 7. In other words, the bucket of the result is determined only by the buckets of the summands.

By now we have come up with a generalization of the concept of parity (for divisibility by 2) to divisibility by 7. Instead of categorizing numbers into even and odd numbers, we categorize them into the 7 buckets depending on their remainder when divided by 7. But we could have chosen any positive integer to start with, not just 7. By using the same techniques we applied above, we can create a new way of analyzing numbers using any positive integer as our base.

4.2 Introducing Multiplication

For simplicity, we'll continue to use 7 as our base, but keep in mind that the interesting results we will notice are valid in other bases also. Above, we saw the important fact that the remainder of the sum of two numbers is the same as the remainder of the sum of the remainders of two numbers. There is a similar fact for multiplication. Indeed,

$$ab \bmod 7 = (a \bmod 7)(b \bmod 7) \bmod 7$$

That is, instead of multiplying two numbers and then taking the remainder of the product, we can instead multiply their remainders and take the remainder of that. While above we gave an algebraic explanation for the sum of two numbers, for the sake of time we will not do that for the product. But a similar algebraic explanation is possible, and if you are interested, you may try to devise it yourself.

We are able to solve advanced problems easily by applying the techniques shown above. Let us consider, for example, the following problems:

Problem 4.2.1 A Million Days

Today is Sunday. 1000 days later, it will be Saturday. 1000000 days later, what day will it be?

Solution:

The question tells us that 1000 days later, it will be Saturday. Since Saturday is 6 days past Sunday, we know that $1000 \bmod 7 = 6$.

We need to compute $1000000 \bmod 7$. We can use the technique developed above to simplify:

$$\begin{aligned} 1000000 \bmod 7 &= (1000 \times 1000) \bmod 7 \\ &= ((1000 \bmod 7) \times (1000 \bmod 7)) \bmod 7 \\ &= (6 \times 6) \bmod 7 \\ &= 36 \bmod 7 \\ &= 1 \end{aligned}$$

so after 1000000 days, the day of the week will be 1 past Sunday, hence $\boxed{\text{Monday}}$.

Problem 4.2.2 A Large Power of 2

Find $2^{32} \bmod 7$.

Solution:

We could find the product, but that would take a long time. Since 16 is a power of 2, it may be useful to consider the remainders of 2^1, 2^2, 2^4, 2^8, 2^{16}, and then finally 2^{32}.

First, note that $2 \bmod 7 = 2$. Then note $2^2 \bmod 7 = 4 \bmod 7 = 4$. Next, note that

$$\begin{aligned} 2^4 \bmod 7 &= (2 \times 2 \times 2 \times 2) \bmod 7 \\ &= 16 \bmod 7 \\ &= 2 \end{aligned}$$

and so far, all the calculations have been short and easy.

For $2^8 \bmod 7$, instead of calculating the product, we could apply the above result:

$$\begin{aligned} 2^8 \bmod 7 &= (\underbrace{2 \times 2 \times \cdots \times 2}_{8 \text{ twos}}) \bmod 7 \\ &= (2 \times 2 \times 2 \times 2)(2 \times 2 \times 2 \times 2) \bmod 7 \\ &= 16 \times 16 \bmod 7 \\ &= (16 \bmod 7)(16 \bmod 7) \bmod 7 \\ &= 2 \times 2 \bmod 7 \\ &= 4 \bmod 7 \\ &= 4 \end{aligned}$$

Next, for $2^{16} \bmod 7$, we do the same thing again:

$$\begin{aligned} 2^{16} \bmod 7 &= (\underbrace{2 \times 2 \times \cdots \times 2}_{16 \text{ twos}}) \bmod 7 \\ &= (\underbrace{2 \times 2 \times \cdots \times 2}_{8 \text{ twos}})(\underbrace{2 \times 2 \times \cdots \times 2}_{8 \text{ twos}}) \bmod 7 \\ &= 2^8 \times 2^8 \bmod 7 \\ &= (2^8 \bmod 7)(2^8 \bmod 7) \bmod 7 \\ &= 4 \times 4 \bmod 7 \\ &= 16 \bmod 7 \\ &= 2 \end{aligned}$$

And finally, one more time for $2^{32} \bmod 7$:

$$\begin{aligned} 2^{32} \bmod 7 &= (\underbrace{2 \times 2 \times \cdots \times 2}_{32 \text{ twos}}) \bmod 7 \\ &= (\underbrace{2 \times 2 \times \cdots \times 2}_{16 \text{ twos}})(\underbrace{2 \times 2 \times \cdots \times 2}_{16 \text{ twos}}) \bmod 7 \\ &= 2^{16} \times 2^{16} \bmod 7 \\ &= (2^{16} \bmod 7)(2^{16} \bmod 7) \bmod 7 \\ &= 2 \times 2 \bmod 7 \\ &= 4 \bmod 7 \\ &= \boxed{4} \end{aligned}$$

4.3 Notation

The kind of computation we were doing above is known as *modular arithmetic*. Sometimes it is convenient to use specialized notation to describe operations. Now we will take look at the commonly used notation, and how it can be used to solve problems.

First, we introduce the concept that two numbers are *congruent* modulo some base k if they have the same remainder when divided by k. For example, 17 and 10 are congruent modulo 7, because $17 \bmod 7 = 3 = 10 \bmod 7$.

We can write this as:

$$17 \equiv 10 \mod 7$$

By working with congruences, we can solve complex problems in relatively few lines of work. For instance, consider the following.

Problem 4.3.1 Huge Number, Small Remainder

Define $10! = 10 \times 9 \times 8 \times \cdots \times 1$. Find $10! \bmod 72$.

Solution: We see that

$$\begin{aligned} 10! &\equiv 10 \times 9 \times 8 \times \cdots \times 1 \mod 72 \\ &\equiv 9 \times 8 \times 10 \times 7 \times 6 \times \cdots \times 1 \mod 72 \\ &\equiv 72 \times 10 \times 7! \mod 72 \\ &\equiv 0 \times 10 \times 7! \mod 72 \\ &\equiv 0 \mod 72 \end{aligned}$$

so $10! \bmod 72 = \boxed{0}$.

4.4 Further Study

We do not have time to further discuss modular arithmetic in this course. But this subject is very powerful, and you will see it again and again in the future.

Glossary

integer a positive or negative whole number, or 0; for example, -8, 2000, or 0. 3

parity decribes whether an integer is even or odd. 3

transitivity the property of certain relations that specifies if an element a is related to b, and the element b is related to c, then a is similarly related to c. 6