Elementary Number Theory

W. Edwin Clark

Department of Mathematics
University of South Florida

Revised June 2, 2003

Preface

Number theory is concerned with properties of the integers:

$$\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots.$$

The great mathematician Carl Friedrich Gauss called this subject *arithmetic* and of it he said:

> Mathematics is the queen of sciences and arithmetic the queen of mathematics."

At first blush one might think that of all areas of mathematics certainly *arithmetic* should be the simplest, but it is a surprisingly deep subject.

We assume that students have some familiarity with basic set theory, and calculus. But very little of this nature will be needed. To a great extent the book is self-contained. It requires only a certain amount of mathematical maturity. And, hopefully, the student's level of mathematical maturity will increase as the course progresses.

Before the course is over students will be introduced to the symbolic programming language Maple which is an excellent tool for exploring number theoretic questions.

If you wish to see other books on number theory, take a look in the QA 241 area of the stacks in our library. One may also obtain much interesting and current information about number theory from the internet. See particularly the websites listed in the Bibliography. The websites by Chris Caldwell [2] and by Eric Weisstein [11] are especially recommended. To see what is going on at the frontier of the subject, you may take a look at some recent issues of the *Journal of Number Theory* which you will find in our library.

Here are some examples of outstanding unsolved problems in number theory. Some of these will be discussed in this course. A solution to any one of these problems would make you quite famous (at least among mathematicians). Many of these problems concern prime numbers. A *prime number* is an integer greater than 1 whose only positive factors are 1 and the integer itself.

1. (*Goldbach's Conjecture*) Every even integer $n > 2$ is the sum of two primes.
2. (*Twin Prime Conjecture*) There are infinitely many twin primes. [If p and $p+2$ are primes we say that p and $p+2$ are *twin primes*.]
3. Are there infinitely many primes of the form $n^2 + 1$?
4. Are there infinitely many primes of the form $2^n - 1$? Primes of this form are called *Mersenne primes*.
5. Are there infinitely many primes of the form $2^{2^n} + 1$? Primes of this form are called *Fermat primes*.
6. ($3n+1$ *Conjecture*) Consider the function f defined for positive integers n as follows: $f(n) = 3n+1$ if n is odd and $f(n) = n/2$ if n is even. The conjecture is that the sequence $f(n), f(f(n)), f(f(f(n))), \cdots$ always contains 1 no matter what the starting value of n is.
7. Are there infinitely many primes whose digits in base 10 are all ones? Numbers whose digits are all ones are called *repunits*.
8. Are there infinitely many perfect numbers? [An integer is *perfect* if it is the sum of its proper divisors.]
9. Is there a fast algorithm for factoring large integers? [A truly fast algoritm for factoring would have important implications for cryptography and data security.]

Famous Quotations Related to Number Theory

Two quotations from G. H. Hardy:

In the first quotation Hardy is speaking of the famous Indian mathematician Ramanujan. This is the source of the often made statement that Ramanujan knew each integer personally.

> I remember once going to see him when he was lying ill at Putney. I had ridden in taxi cab number 1729 and remarked that the number seemed to me rather a dull one, and that I hoped it was not an unfavorable omen. "No," he replied, "it is a very interesting number; it is the smallest number expressible as the sum of two cubes in two different ways. "

> Pure mathematics is on the whole distinctly more useful than applied. For what is useful above all is technique, and mathematical technique is taught mainly through pure mathematics.

Two quotations by Leopold Kronecker

> God has made the integers, all the rest is the work of man.

The original quotation in German was *Die ganze Zahl schuf der liebe Gott, alles Übrige ist Menschenwerk.* More literally, the translation is " The whole number, created the dear God, everything else is man's work." Note in particular that *Zahl* is German for *number*. This is the reason that today we use $\mathbb{Z}$ for the set of integers.

> Number theorists are like lotus-eaters – having once tasted of this food they can never give it up.

A quotation by contemporary number theorist William Stein:

> A computer is to a number theorist, like a telescope is to an astronomer. It would be a shame to teach an astronomy class without touching a telescope; likewise, it would be a shame to teach this class without telling you how to look at the integers through the lens of a computer.

Contents

Chapter 1

Basic Axioms for $\mathbb{Z}$

Since number theory is concerned with properties of the integers, we begin by setting up some notation and reviewing some basic properties of the integers that will be needed later:

$$\begin{aligned}
&\mathbb{N} = \{1, 2, 3, \cdots\} \quad \text{(the } \textbf{natural numbers} \text{ or } \textbf{positive integers}\text{)}\\
&\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\} \quad \text{(the } \textbf{integers}\text{)}\\
&\mathbb{Q} = \left\{\frac{n}{m} \mid n, m \in \mathbb{Z} \text{ and } m \neq 0\right\} \quad \text{(the } \textbf{rational numbers}\text{)}\\
&\mathbb{R} = \text{the } \textbf{real numbers}
\end{aligned}$$

Note that $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$. I assume a knowledge of the basic rules of high school algebra which apply to $\mathbb{R}$ and therefore to $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$. By this I mean things like $ab = ba$ and $ab + ac = a(b + c)$. I will not list all of these properties here. However, below I list some particularly important properties of $\mathbb{Z}$ that will be needed. I call them *axioms* since we will not prove them in this course.

Some Basic Axioms for $\mathbb{Z}$

1. If a, $b \in \mathbb{Z}$, then $a + b$, $a - b$ and $ab \in \mathbb{Z}$. ($\mathbb{Z}$ is closed under addition, subtraction and multiplication.)

2. If $a \in \mathbb{Z}$ then there is no $x \in \mathbb{Z}$ such that $a < x < a + 1$.

3. If a, $b \in \mathbb{Z}$ and $ab = 1$, then either $a = b = 1$ or $a = b = -1$.

4. **Laws of Exponents:** For n, m in $\mathbb{N}$ and a, b in $\mathbb{R}$ we have

(a) $(a^n)^m = a^{nm}$

(b) $(ab)^n = a^n b^n$

(c) $a^n a^m = a^{n+m}$.

These rules hold for all $n, m \in \mathbb{Z}$ if a and b are not zero.

5. **Properties of Inequalities:** For a, b, c in $\mathbb{R}$ the following hold:

   (a) (*Transitivity*) If $a < b$ and $b < c$, then $a < c$.

   (b) If $a < b$ then $a + c < b + c$.

   (c) If $a < b$ and $0 < c$ then $ac < bc$.

   (d) If $a < b$ and $c < 0$ then $bc < ac$.

   (e) (*Trichotomy*) Given a and b, one and only one of the following holds:
   $$a = b, \quad a < b, \quad b < a.$$

6. **The Well-Ordering Property for $\mathbb{N}$:** Every non-empty subset of $\mathbb{N}$ contains a least element.

7. **The Principle of Mathematical Induction:** Let $P(n)$ be a statement concerning the integer variable n. Let n_0 be any fixed integer. $P(n)$ is true for all integers $n \geq n_0$ if one can establish both of the following statements:

   (a) $P(n)$ is true if $n = n_0$.

   (b) Whenever $P(n)$ is true for $n_0 \leq n \leq k$ then $P(n)$ is true for $n = k + 1$.

We use the usual conventions:

1. $a \leq b$ means $a < b$ or $a = b$,

2. $a > b$ means $b < a$, and

3. $a \geq b$ means $b \leq a$.

Important Convention. Since in this course we will be almost exclusively concerned with integers we shall assume from now on (unless otherwise stated) that all lower case roman letters $a, b, \ldots, z$ are integers.

Chapter 2

Proof by Induction

In this section, I list a number of statements that can be proved by use of The Principle of Mathematical Induction. I will refer to this principle as *PMI* or, simply, *induction*. A sample proof is given below. The rest will be given in class *hopefully by students.*

A sample proof using induction: I will give two versions of this proof. In the first proof I explain in detail how one uses the PMI. The second proof is less pedagogical and is the type of proof I expect students to construct. I call the statement I want to prove a *proposition*. It might also be called a *theorem, lemma* or *corollary* depending on the situation.

Proposition 2.1. *If* $n \geq 5$ *then* $2^n > 5n$.

Proof #1. Here we use The Principle of Mathematical Induction. Note that PMI has two parts which we denote by PMI (a) and PMI (b).

We let $P(n)$ be the statement $2^n > 5n$. For n_0 we take 5. We could write simply:

$$P(n) = 2^n > 5n \text{ and } n_0 = 5.$$

Note that $P(n)$ represents a *statement*, usually an inequality or an equation but sometimes a more complicated assertion. Now if $n = 4$ then $P(n)$ becomes the statement $2^4 > 5 \cdot 4$ which is false! But if $n = 5$, $P(n)$ is the statement $2^5 > 5 \cdot 5$ or $32 > 25$ which is true and we have established PMI (a).

Now to prove PMI (b) we begin by *assuming* that

$$P(n) \text{ is true for } 5 \leq n \leq k.$$

That is, we assume

$$2^n > 5n \text{ for } 5 \leq n \leq k. \tag{2.1}$$

The assumption (2.1) is called the **induction hypothesis**. We want to use it to prove that $P(n)$ holds when $n = k + 1$. So here's what we do. By (2.1) letting $n = k$ we have

$$2^k > 5k.$$

Multiply both sides by two and we get

$$2^{k+1} > 10k. \tag{2.2}$$

Note that we are trying to prove $2^{k+1} > 5(k + 1)$. Now $5(k + 1) = 5k + 5$ so if we can show $10k \geq 5k + 5$ we can use (2.2) to complete the proof.

Now $10k = 5k + 5k$ and $k \geq 5$ by (2.1) so $k \geq 1$ and hence $5k \geq 5$. Therefore

$$10k = 5k + 5k \geq 5k + 5 = 5(k + 1).$$

Thus

$$2^{k+1} > 10k \geq 5(k + 1)$$

so

$$2^{k+1} > 5(k + 1). \tag{2.3}$$

that is, $P(n)$ holds when $n = k + 1$. So assuming the induction hypothesis (2.1) we have proved (2.3). Thus we have established PMI (b).

We have established that parts (a) and (b) of PMI hold for this particular $P(n)$ and n_0. So the PMI tells us that $P(n)$ holds for $n \geq 5$. That is, $2^n > 5n$ holds for $n \geq 5$. □

I now give a more streamlined proof.

Proposition 2.2. *If $n \geq 5$ then $2^n > 5n$.*

Proof #2. We prove the proposition by induction on the variable n.
If $n = 5$ we have $2^5 > 5 \cdot 5$ or $32 > 25$ which is true.
Assume

$$2^n > 5n \quad \text{for } 5 \leq n \leq k \quad \text{(the induction hypothesis)}.$$

Taking $n = k$ we have

$$2^k > 5k.$$

Multiplying both sides by 2 gives

$$2^{k+1} > 10k.$$

Now $10k = 5k + 5k$ and $k \geq 5$ so $k \geq 1$ and therefore $5k \geq 5$. Hence

$$10k = 5k + 5k \geq 5k + 5 = 5(k+1).$$

It follows that

$$2^{k+1} > 10k \geq 5(k+1)$$

and therefore

$$2^{k+1} > 5(k+1).$$

Hence by PMI we conclude that $2^n > 5n$ for $n \geq 5$. □

The 8 major parts of a proof by induction:

1. First state what proposition you are going to prove. Precede the statement by *Proposition, Theorem, Lemma, Corollary, Fact,* or *To Prove:*.

2. Write the *Proof* or *Pf.* at the very beginning of your proof.

3. Say that you are going to use induction (some proofs do not use induction!) and if it is not obvious from the statement of the proposition identify clearly $P(n)$, the statement to be proved, the variable n and the starting value n_0. Even though this is usually clear, sometimes these things may not be obvious. And, of course, the variable need not be n. It could be represented in many different ways.

4. Prove that $P(n)$ holds when $n = n_0$.

5. Assume that $P(n)$ holds for $n_0 \leq n \leq k$. This assumption will be referred to as the *induction hypothesis*.

6. Use the induction hypothesis and anything else that is known to be true to prove that $P(n)$ holds when $n = k + 1$.

7. Conclude that since the conditions of the PMI have been met then $P(n)$ holds for $n \geq n_0$.

8. Write QED or ■ or // or something to indicate that you have completed your proof.

Exercise 2.1. Prove that $2^n > 6n$ for $n \geq 5$.

Exercise 2.2. Prove that $1 + 2 + \cdots + n = \dfrac{n(n+1)}{2}$ for $n \geq 1$.

Exercise 2.3. Prove that if $0 < a < b$ then $0 < a^n < b^n$ for all $n \in \mathbb{N}$.

Exercise 2.4. Prove that $n! < n^n$ for $n \geq 2$.

Exercise 2.5. Prove that if a and r are real numbers and $r \neq 1$, then for $n \geq 1$

$$a + ar + ar^2 + \cdots + ar^n = \frac{a\left(r^{n+1} - 1\right)}{r - 1}.$$

This can be written as follows

$$a(r^{n+1} - 1) = (r - 1)(a + ar + ar^2 + \cdots + ar^n).$$

And important special case of which is

$$(r^{n+1} - 1) = (r - 1)(1 + r + r^2 + \cdots + r^n).$$

Exercise 2.6. Prove that $1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$ for $n \geq 1$.

Exercise 2.7. Prove that $\underbrace{111\cdots1}_{n\,1\text{'s}} = \dfrac{10^n - 1}{9}$ for $n \geq 1$.

Exercise 2.8. Prove that $1^2 + 2^2 + 3^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$ if $n \geq 1$.

Exercise 2.9. Prove that if $n \geq 12$ then n can be written as a sum of 4's and 5's. For example, $23 = 5 + 5 + 5 + 4 + 4 = 3 \cdot 5 + 2 \cdot 4$. *[Hint. In this case it will help to do the cases $n = 12$, 13, 14, and 15 separately. Then use induction to handle $n \geq 16$.]*

Exercise 2.10. (a) For $n \geq 1$, the *triangular number* t_n is the number of dots in a triangular array that has n rows with i dots in the i-th row. Find a formula for t_n, $n \geq 1$. (b) Suppose that for each $n \geq 1$. Let s_n be the number of dots in a square array that has n rows with n dots in each row. Find a formula for s_n. The numbers s_n are usually called *squares*.

Exercise 2.11. Find the first 10 triangular numbers and the first 10 squares. Which of the triangular numbers in your list are also squares? Can you find the next triangular number which is a square?

Exercise 2.12. Some propositions that can be proved by induction can also be proved without induction. Prove Exercises 2.2 and 2.5 without induction. *[Hints: For* 2.2 *write* $s = 1+2+\cdots+(n-1)+n$*. Directly under this equation write* $s = n+(n-1)+\cdots+2+1$*. Add these equations to obtain* $2s = n(n+1)$*. Solve for* s*. For Exercise* 2.5 *write* $p = a+ar+ar^2+\cdots+ar^n$*. Then multiply both sides of this equation by* r *to get a new equation with* rp *as the left hand side. Subtract these two equation to obtain* $pr - p = ar^{n+1} - a$*. Now solve for* p*.]*

Chapter 3

Elementary Divisibility Properties

Definition 3.1. $d \mid n$ means there is an integer k such that $n = dk$. $d \nmid n$ means that $d \mid n$ is false.

Note that $a \mid b \neq a/b$. Recall that a/b represents the fraction $\frac{a}{b}$.
The expression $d \mid n$ may be read in any of the following ways:

1. d *divides* n.
2. d is a *divisor* of n.
3. d is a *factor* of n.
4. n is a *multiple* of d.

Thus, the following five statements are equivalent, that is, they are all different ways of saying the same thing.

1. $2 \mid 6$.
2. 2 divides 6.
3. 2 is a divisor of 6.
4. 2 is a factor of 6.
5. 6 is a multiple of 2.

Definitions will play an important role in this course. Students should learn all definitions and be able to state them precisely. An alternative way to state the definition of $d \mid n$ is as follows.

Definition 3.2. $d \mid n \iff n = dk \text{ for some } k.$

or maybe

Definition 3.3. $d \mid n$ iff $n = dk$ for some k.

Keep in mind that we are assuming that all letters $a, b, \ldots, z$ represent integers. Otherwise we would have to add this fact to our definitions. One might also see the following definition sometimes.

Definition 3.4. $d \mid n$ if $n = dk$ for some k.

Note that $\iff$, *iff*, and *if and only if*, all mean the same thing. In definitions such as Definition 3.4 *if* is interpreted to mean *if and only if*. It should be emphasized that all the above definitions are acceptable. Take your pick. But be careful about making up your own definitions.

Theorem 3.1 (Divisibility Properties). *If n, m, and d are integers then the following statements hold:*

1. $n \mid n$ (*everything divides itself*)
2. $d \mid n$ *and* $n \mid m \implies d \mid m$ (*transitivity*)
3. $d \mid n$ *and* $d \mid m \implies d \mid an + bm$ *for all a and b* (*linearity property*)
4. $d \mid n \implies ad \mid an$ (*multiplication property*)
5. $ad \mid an$ *and* $a \neq 0 \implies d \mid n$ (*cancellation property*)
6. $1 \mid n$ (*one divides everything*)
7. $n \mid 1 \implies n = \pm 1$ (1 *and* -1 *are the only divisors of* 1.)
8. $d \mid 0$ (*everything divides zero*)
9. $0 \mid n \implies n = 0$ (*zero divides only zero*)
10. *If d and n are positive and $d \mid n$ then $d \leq n$* (*comparison property*)

Exercise 3.1. Prove each of the properties 1 through 10 in Theorem 3.1.

Definition 3.5. If $c = as + bt$ for some integers s and t we say that c is a **linear combination** of a and b.

Thus, statement 3 in Theorem 3.1 says that if d divides a and b, then d divides all linear combinations of a and b. In particular, d divides $a + b$ and $a - b$. This will turn out to be a useful fact.

Exercise 3.2. Prove that if $d \mid a$ and $d \mid b$ then $d \mid a - b$.

Exercise 3.3. Prove that if $a \in \mathbb{Z}$ then the only positive divisor of both a and $a + 1$ is 1.

Chapter 4

The Floor and Ceiling of a Real Number

Here we define the floor, *a.k.a.*, the greatest integer, and the ceiling, *a.k.a.*, the least integer, functions. Kenneth Iverson introduced this notation and the terms *floor* and *ceiling* in the early 1960s — according to Donald Knuth [6] who has done a lot to popularize the notation. Now this notation is standard in most areas of mathematics.

Definition 4.1. If x is any real number we define

$$\lfloor x \rfloor = \text{ the greatest integer less than or equal to } x$$

$$\lceil x \rceil = \text{ the least integer greater than or equal to } x$$

$\lfloor x \rfloor$ is called the **floor** of x and $\lceil x \rceil$ is called the **ceiling** of x The floor $\lfloor x \rfloor$ is sometimes denoted $[x]$ and called the greatest integer function. But I prefer the notation $\lfloor x \rfloor$. Here are a few simple examples:

1. $\lfloor 3.1 \rfloor = 3$ and $\lceil 3.1 \rceil = 4$
2. $\lfloor 3 \rfloor = 3$ and $\lceil 3 \rceil = 3$
3. $\lfloor -3.1 \rfloor =$ -4 and $\lceil -3.1 \rceil =$ -3

From now on we mostly concentrate on the floor $\lfloor x \rfloor$. For a more detailed treatment of both the floor and ceiling see the book **Concrete Mathematics** [5]. According to the definition of $\lfloor x \rfloor$ we have

$$\lfloor x \rfloor = \max\{n \in \mathbb{Z} \mid n \leq x\} \tag{4.1}$$

Note also that if n is an integer we have:

$$n = \lfloor x \rfloor \Longleftrightarrow n \le x < n + 1. \tag{4.2}$$

From this it is clear that

$$\lfloor x \rfloor \le x \text{ holds for all } x,$$

and

$$\lfloor x \rfloor = x \Longleftrightarrow x \in \mathbb{Z}.$$

We need the following lemma to prove our next theorem.

Lemma 4.1. *For all $x \in \mathbb{R}$*

$$x - 1 < \lfloor x \rfloor \le x.$$

Proof. Let $n = \lfloor x \rfloor$. Then by (4.2) we have $n \le x < n + 1$. This gives immediately that $\lfloor x \rfloor \le x$, as already noted above. It also gives $x < n + 1$ which implies that $x - 1 < n$, that is, $x - 1 < \lfloor x \rfloor$. □

Exercise 4.1. Sketch the graph of the function $f(x) = \lfloor x \rfloor$ for $-3 \le x \le 3$.

Exercise 4.2. Find $\lfloor \pi \rfloor$, $\lceil \pi \rceil$, $\lfloor \sqrt{2} \rfloor$, $\lceil \sqrt{2} \rceil$, $\lfloor -\pi \rfloor$, $\lceil -\pi \rceil$, $\lfloor -\sqrt{2} \rfloor$, and $\lceil -\sqrt{2} \rceil$.

Definition 4.2. Recall that the **decimal representation** of a positive integer a is given by $a = a_{n-1}a_{n-2}\cdots a_1a_0$ where

$$a = a_{n-1}10^{n-1} + a_{n-2}10^{n-2} + \cdots + a_1 10 + a_0 \tag{4.3}$$

and the *digits* $a_{n-1}, a_{n-2}, \ldots, a_1, a_0$ are in the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ with $a_{n-1} \ne 0$. In this case we say that **the integer a is an n digit number** or that a **is n digits long.**

Exercise 4.3. Prove that $a \in \mathbb{N}$ is an n digit number where $n = \lfloor \log(a) \rfloor + 1$. Here log means logarithm to base 10. *Hint: Show that if (4.3) holds with $a_{n-1} \ne 0$ then $10^{n-1} \le a < 10^n$. Then apply the* log *to all terms of this inequality.*

Exercise 4.4. Use the previous exercise to determine the number of digits in the decimal representation of the number $2^{3321928}$. *Recall that* $\log(x^y) = y\log(x)$ *when x and y are positive.*

Chapter 5

The Division Algorithm

The goal of this section is to prove the following important result.

Theorem 5.1 (The Division Algorithm). *If a and b are integers and $b > 0$ then there exist unique integers q and r satisfying the two conditions:*

$$a = bq + r \quad \textit{and} \quad 0 \leq r < b. \tag{5.1}$$

In this situation q is called the *quotient* and r is called the *remainder* when *a is divided by b*. Note that there are two parts to this result. One part is the EXISTENCE of integers q and r satisfying (5.1) and the second part is the UNIQUENESS of the integers q and r satisfying (5.1).

Proof. Given $b > 0$ and any a define

$$\begin{aligned} q &= \left\lfloor \frac{a}{b} \right\rfloor \\ r &= a - bq \end{aligned}$$

Cleary we have $a = bq + r$. But we need to prove that $0 \leq r < b$. By Lemma 4.1 we have

$$\frac{a}{b} - 1 < \left\lfloor \frac{a}{b} \right\rfloor \leq \frac{a}{b}.$$

Now multiply all terms of this inequality by $-b$. Since b is positive, $-b$ is negative so the direction of the inequality is reversed, giving us:

$$b - a > -b \left\lfloor \frac{a}{b} \right\rfloor \geq -a.$$

If we add a to all sides of the inequality and replace $\lfloor a/b \rfloor$ by q we obtain

$$b > a - bq \geq 0.$$

Since $r = a - bq$ this gives us the desired result $0 \leq r < b$.

We still have to prove that q and r are uniquely determined. To do this we assume that

$$a = bq_1 + r_1 \quad \text{and} \quad 0 \leq r_1 < b,$$

and

$$a = bq_2 + r_2 \quad \text{and} \quad 0 \leq r_2 < b.$$

We must show that $r_1 = r_2$ and $q_1 = q_2$. If $r_1 \neq r_2$ without loss of generality we can assume that $r_2 > r_1$. Subtracting these two equations we obtain

$$0 = a - a = (bq_1 + r_1) - (bq_2 + r_2) = b(q_1 - q_2) + (r_1 - r_2).$$

This implies that

$$r_2 - r_1 = b(q_1 - q_2). \tag{5.2}$$

This implies that $b \mid r_2 - r_1$. By Theorem 3.1(10) this implies that $b \leq r_2 - r_1$. But since

$$0 \leq r_1 < r_2 < b$$

we have $r_2 - r_1 < b$. This contradicts $b \leq r_2 - r_1$. So we must conclude that $r_1 = r_2$. Now from (5.2) we have $0 = b(q_1 - q_2)$. Since $b > 0$ this tells us that $q_1 - q_2 = 0$, that is, $q_1 = q_2$. This completes the proof of the uniqueness of r and q in (5.1). □

Definition 5.1. An integer n is *even* if $n = 2k$ for some k, and is *odd* if $n = 2k + 1$ for some k.

Exercise 5.1. Prove using the Division Algorithm that every integer is either even or odd, but never both.

Definition 5.2. By the *parity* of an integer we mean whether it is even or odd.

Exercise 5.2. Prove n and n^2 always have the same parity. That is, n is even if and only if n^2 is even.

Exercise 5.3. Find the q and r of the Division Algorithm for the following values of a and b:

1. Let $b = 3$ and $a = 0, 1, -1, 10, -10$.

2. Let $b = 345$ and $a = 0, -1, 1, 344, 7863, -7863$.

Exercise 5.4. Devise a method for solving problems like those in the previous exercise for large positive values of a and b using a calculator. Illustrate by using $a = 123456$ and $b = 123$. *Hint: If $a = bq + r$ and $0 \leq r < b$ then $\frac{a}{b} = q + \frac{r}{b}$ and so $\frac{r}{b}$ is the fractional part of the decimal number $\frac{a}{b}$. So q is what you get when you drop the fractional part. Once you have q you can solve $a = bq + r$ for r.*

Sometimes a problem in number theory can be solved by dividing the integers into various classes depending on their remainders when divided by some number b. For example, this is helpful in solving the following two problems.

Exercise 5.5. Show that for all integers n the number $n^3 - n$ always has 3 as a factor. (Consider the three cases: $n = 3k$, $n = 3k + 1$, $n = 3k + 2$.)

Exercise 5.6. Show that the product of any three consecutive integers has 6 as a factor. (How many cases should you use here?)

Definition 5.3. For $b > 0$ define $a \bmod b = r$ where r is the remainder given by the Division Algorithm when a is divided by b, that is, $a = bq + r$ and $0 \leq r < b$.

For example $23 \bmod 7 = 2$ since $23 = 7 \cdot 3 + 2$ and $-4 \bmod 5 = 1$ since $-4 = 5 \cdot (-1) + 1$.

Note that some calculators and most programming languages have a function often denoted by $MOD(a, b)$ or $mod(a, b)$ whose value is what we have just defined as $a \bmod b$. When this is the case the values r and q in the Division Algorithm for given a and $b > 0$ are given by

$$r = a \bmod b$$
$$q = \frac{a - (a \bmod b)}{b}$$

If also the floor function is available we have

$$r = a \bmod b$$
$$q = \lfloor a/b \rfloor$$

Exercise 5.7. Prove that if $b > 0$ then $b \mid a \iff a \bmod b = 0$.

Exercise 5.8. Prove that if $b \neq 0$ then $b \mid a \iff a/b \in \mathbb{Z}$.

Exercise 5.9. Calculate the following:

1. $0 \bmod 10$
2. $123 \bmod 10$
3. $10 \bmod 123$
4. $457 \bmod 33$
5. $(-7) \bmod 3$
6. $(-3) \bmod 7$
7. $(-5) \bmod 5$

Exercise 5.10. Use the Division Algorithm to prove the following more general version: If $b \neq 0$ then for any a there exists unique q and r such that

$$a = bq + r \quad \text{and} \quad 0 \leq r < |\,b\,|. \tag{5.3}$$

Hint: Recall that $|\,b\,|$ is b if $b \geq 0$ and is $-b$ if $b < 0$. We know the statement holds if $b > 0$ so we only need to consider the case when $b < 0$. If b is negative then $-b$ is positive, so we can apply the Division Algorithm to a and $-b$. Note that a as well as q can be any integers. This exercise may come in handy later.

Chapter 6

Greatest Common Divisor

Definition 6.1. Let $a, b \in \mathbb{Z}$. If $a \neq 0$ or $b \neq 0$, we define $\gcd(a, b)$ to be the largest integer d such that $d \mid a$ and $d \mid b$. We define $\gcd(0, 0) = 0$.

Discussion. If $e \mid a$ and $e \mid b$ we call e a *common divisor of* a *and* b. Let

$$C(a, b) = \{e : e \mid a \text{ and } e \mid b\},$$

that is, $C(a, b)$ is the set of *all* common divisors of a and b. Note that since everything divides 0

$$C(0, 0) = \mathbb{Z}$$

so there is no largest common divisor of 0 with 0. This is why we must *define* $\gcd(0, 0) = 0$.

Example 6.1.

$$C(18, 30) = \{-1, 1, -2, 2, -3, 3, -6, 6\}.$$

So $\gcd(18, 30) = 6$.

Lemma 6.1. *If* $e \mid a$ *then* $-e \mid a$.

Proof. If $e \mid a$ then $a = ek$ for some k. Then $a = (-e)(-k)$. Since $-e$ and $-k$ are also integers $-e \mid a$. $\square$

Lemma 6.2. *If* $a \neq 0$, *the largest positive integer that divides* a *is* $|a|$.

Proof. Recall that

$$|a| = \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a < 0. \end{cases}$$

First note that $|a|$ actually divides a: If $a > 0$, since we know $a \mid a$ we have $|a| \mid a$. If $a < 0$, $|a| = -a$. In this case $a = (-a)(-1) = |a|(-1)$ so $|a|$ is a factor of a. So, in either case $|a|$ divides a, and in either case $|a| > 0$, since $a \neq 0$.

Now suppose $d \mid a$ and d is positive. Then $a = dk$ some k so $-a = d(-k)$ for some k. So $d \mid |a|$. So by Theorem 3.1 (10) we have $d \leq |a|$. □

The following lemma shows that in computing gcd's we may restrict ourselves to the case where both integers are positive.

Lemma 6.3. $\gcd(a, b) = \gcd(|a|, |b|)$.

Proof. If $a = 0$ and $b = 0$, we have $|a| = a$ and $|b| = b$. So $\gcd(a, b) = \gcd(|a|, |b|)$. Suppose one of a or b is not 0. Note that $d \mid a \Leftrightarrow d \mid |a|$. See Exercise 6.1. It follows that

$$C(a, b) = C(|a|, |b|).$$

So the largest common divisor of a and b is also the largest common divisor of $|a|$ and $|b|$. □

Exercise 6.1. Prove that

$$d \mid a \Leftrightarrow d \mid |a|$$

[Hint: recall that $|a| = a$ if $a \geq 0$ and $|a| = -a$ if $a < 0$. So you need to consider two cases.]

Lemma 6.4. $\gcd(a, b) = \gcd(b, a)$.

Proof. Clearly $C(a, b) = C(b, a)$. It follows that the largest integer in $C(a, b)$ is the largest integer in $C(b, a)$, that is, $\gcd(a, b) = \gcd(b, a)$. □

Lemma 6.5. *If $a \neq 0$ and $b \neq 0$, then $\gcd(a, b)$ exists and satisfies*

$$0 < \gcd(a, b) \leq \min\{|a|, |b|\}.$$

Proof. Note that $\gcd(a,b)$ is the largest integer in the set $C(a,b)$ of common division of a and b. Since $1 \mid a$ and $1 \mid b$ we know that $1 \in C(a,b)$. So the largest common divisor must be at least 1 and is therefore positive. On the other hand $d \in C(a,b) \Rightarrow d \mid |a|$ and $d \mid |b|$ so d is no larger than $|a|$ and no larger than $|b|$. So d is at most the smaller of $|a|$ and $|b|$. Hence $\gcd(a,b) \leq \min\{|a|,|b|\}$. □

Example 6.2. From the above lemmas we have

$$\begin{aligned}\gcd(48,732) &= \gcd(-48,732)\\ &= \gcd(-48,-732)\\ &= \gcd(48,-732).\end{aligned}$$

We also know that

$$0 < \gcd(48,732) \leq 48.$$

Since if $d = \gcd(48,732)$, then $d \mid 48$, to find d we may check only which positive divisors of 48 also divide 732.

Exercise 6.2. Find $\gcd(48,732)$ using Example 6.2.

Exercise 6.3. Find $\gcd(a,b)$ for each of the following values of a and b:

(1) $a = -b$, $b = 14$

(2) $a = -1$, $b = 78654$

(3) $a = 0$, $b = -78$

(4) $a = 2$, $b = -786541$

Chapter 7

The Euclidean Algorithm

Unlike the Division Algorithm, the Euclidean Algorithm *really is* an algorithm. It provides a method to compute $\gcd(a, b)$. Since as already noted $\gcd(0, 0) = 0$, $\gcd(a, b) = \gcd(|a|, |b|)$, and $\gcd(a, b) = \gcd(b, a)$, it suffices to give a method to compute $\gcd(a, b)$ when $a \geq b \geq 0$.

Lemma 7.1. *If* $a > 0$*, then* $\gcd(a, 0) = a$.

Proof. Since every integer divides 0, $C(a, 0)$ is just the set of divisors of a. By Lemma 6.2 the largest divisor of a is $|a|$. Since $a > 0$, $|a| = a$. This shows that $\gcd(a, 0) = a$. $\square$

Remark 7.1. So we are now reduced to the problem of finding $\gcd(a, b)$ when $a \geq b > 0$.

Exercise 7.1. Prove that if $a > 0$ then $\gcd(a, a) = a$.

Now having done Exercise 7.1 we only need to consider the case $a > b > 0$.

Lemma 7.2. *Let* $a > b > 0$*. If* $a = bq + r$*, then*

$$\gcd(a, b) = \gcd(b, r).$$

Proof. It suffices to show that $C(a, b) = C(b, r)$, that is, the common divisors of a and b are the same as the common divisors of b and r. To show this first let $d \mid a$ and $d \mid b$. Note that $r = a - bq$, which is a linear combination of a and b. So by Theorem 3.1(3) $d \mid r$. Thus $d \mid b$ and $d \mid r$. Next assume $d \mid b$ and $d \mid r$. Using Theorem 3.1(3) again and the fact that $a = bq + r$ is a linear combination of b and r, we have $d \mid a$. So $d \mid a$ and $d \mid b$. We have thus shown that $C(a, b) = C(b, r)$. So $\gcd(a, b) = \gcd(b, r)$. $\square$

Remark 7.2. The **Euclidean Algorithm** is the process of using Lemmas 7.2 and 7.1 to compute $\gcd(a, b)$ when $a > b > 0$.

Rather than give a precise statement of the algorithm I will give an example to show how it goes.

Example 7.1. Let's compute $\gcd(803, 154)$.

$$\begin{aligned}
\gcd(803, 154) &= \gcd(154, 33) \quad \text{since } 803 = 154 \cdot 5 + 33 \\
\gcd(154, 33) &= \gcd(33, 22) \quad \text{since } 154 = 33 \cdot 4 + 22 \\
\gcd(33, 22) &= \gcd(22, 11) \quad \text{since } 33 = 22 \cdot 1 + 11 \\
\gcd(22, 11) &= \gcd(11, 0) \quad \text{since } 22 = 11 \cdot 2 + 0 \\
\gcd(11, 0) &= 11.
\end{aligned}$$

Hence $\gcd(803, 154) = 11$.

Remark 7.3. Note that we have formed the gcd of 803 and 154 *without* factoring 803 and 154. This method is generally much faster than factoring and can find gcd's when factoring is not feasible.

Exercise 7.2. Let $a > b > 0$. Show that $\gcd(a, b) = \gcd(b, a \bmod b)$.

Remark 7.4. So if your calculator can compute $a \bmod b$ you may use it when executing the Euclidean Algorithm.

Exercise 7.3. Find $\gcd(a, b)$ *using the Euclidean Algorithm* for each of the values below:

(1) $a = 37$, $b = 60$

(2) $a = 793$, $b = 3172$

(3) $a = 25174$, $b = 42722$

(4) $a = 377$, $b = 233$

Chapter 8

Bezout's Lemma

Lemma 8.1 (Bezout's Lemma). *For all integers a and b there exist integers s and t such that*

$$\gcd(a, b) = sa + tb.$$

Proof. If $a = b = 0$ then s and t may be anything since

$$\gcd(0, 0) = 0 = s \cdot 0 + t \cdot 0.$$

So we may assume that $a \neq 0$ or $b \neq 0$. Let

$$J = \{na + mb : n, m \in \mathbb{Z}\}.$$

Note that J contains a, $-a$, b and $-b$ since

$$\begin{aligned} a &= 1 \cdot a + 0 \cdot b \\ -a &= (-1) \cdot a + 0 \cdot b \\ b &= 0 \cdot a + 1 \cdot b \\ -b &= 0 \cdot a + (-1) \cdot b. \end{aligned}$$

Since $a \neq 0$ or $b \neq 0$ one of the elements a, $-a$, b, $-b$ is positive. So we can say that J contains some positive integers. Let S denote the set of positive integers in J. That is,

$$S = \{na + mb : na + mb > 0,\ n, m \in \mathbb{Z}\}.$$

By the Well-Ordering Property for $\mathbb{N}$, S contains a smallest positive integer, call it d. Let's show that $d = \gcd(a, b)$. Note that since $d \in S$ we have

$d = sa+tb$ for some integers, s and t. Note also that $d > 0$. Let $e = \gcd(a, b)$. Then $e \mid a$ and $e \mid b$, so by Theorem 3.1 (3) $e \mid sa + tb$, that is $e \mid d$. Since e and d are positive, by Theorem 3.1 (10) we have $e \leq d$. So if we can show that d is a common divisor of a and b we will know that $e = d$. To show $d \mid a$ using the Division Algorithm we write $a = dq + r$ where $0 \leq r < d$. Now

$$\begin{aligned} r &= a - dq \\ &= a - (sa + tb)q \\ &= (1 - sq)a + (-tq)b. \end{aligned}$$

Hence $r \in J$. If $r > 0$ then $r \in S$. But this cannot be since $r < d$ and d is the smallest integer in S. So we must have $r = 0$. That is, $a = dq$. Hence $d \mid a$. By a similar argument we can show that $d \mid b$. Thus, d is indeed a common divisor of a and b since $d \geq e = \gcd(a, b)$, we must have $d = \gcd(a, b)$. As noted already $d = sa + tb$, so the theorem is proved. $\square$

Example 8.1. $1 = \gcd(2, 3)$ and we have $1 = (-1)2 + 1 \cdot 3$. Also we have $1 = 2 \cdot 2 + (-1)3$. So the numbers s and t in Bezout's Lemma are *not* uniquely determined. In fact, as we will see later there are *infinitely* many choices for s and t for each pair a, b.

Remark 8.1. The above proof is an *existence* theorem. It asserts the existence of s and t, but does not provide a way to actually find s and t. Also *the proof* does not give any clue about how to go about calculating s and t. We will give an algorithm in the next chapter for finding s and t.

Chapter 9

Blankinship's Method

In an article in the August-September 1963 issue of the *American Mathematical Monthly*, W.A. Blankinship[1] gave a simple method to produce the integers s and t in Bezout's Lemma and at the same time produce $\gcd(a, b)$:

Given $a > b > 0$ we start with the array

$$\begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$$

Then we continue to add multiples of one row to another row, alternating choice of rows until we reach an array of the form

$$\begin{bmatrix} 0 & x_1 & x_2 \\ d & y_1 & y_2 \end{bmatrix}$$

or

$$\begin{bmatrix} d & y_1 & y_2 \\ 0 & x_1 & x_2 \end{bmatrix}$$

Then $d = \gcd(a, b) = y_1 a + y_2 b$. [The goal is to get a 0 in the first column.]

Examples 9.1. First take $a = 35$, $b = 15$.

$$\begin{bmatrix} 35 & 1 & 0 \\ 15 & 0 & 1 \end{bmatrix}$$

Note $35 = 15 \cdot 2 + 5$, hence

$$35 + 15(-2) = 5.$$

[1]Thanks to Chris Miller for bringing this method to my attention.

So we multiply row 2 by -2 and add it to row 1, getting

$$\begin{bmatrix} 5 & 1 & -2 \\ 15 & 0 & 1 \end{bmatrix}$$

Now $3 \cdot 5 = 15$ or $15 + (-3)5 = 0$, so we multiply row 1 by -3 and add it to row 2, getting

$$\begin{bmatrix} 5 & 1 & -2 \\ 0 & -3 & 7 \end{bmatrix}.$$

Now we can say that

$$\boxed{\gcd(35, 15) = 5}$$

and

$$\boxed{5 = 1 \cdot 35 + (-2) \cdot 15.}$$

Let's now consider a more complicated example: Take $a = 1876$, $b = 365$.

$$\begin{bmatrix} 1876 & 1 & 0 \\ 365 & 0 & 1 \end{bmatrix}$$

Now $1876 = 365 \cdot 5 + 51$ so we add -5 times the second row to the first row, getting:

$$\begin{bmatrix} 51 & 1 & -5 \\ 365 & 0 & 1 \end{bmatrix}$$

Now $365 = 51 \cdot 7 + 8$, so we add -7 times row 1 to row 2, getting:

$$\begin{bmatrix} 51 & 1 & -5 \\ 8 & -7 & 36 \end{bmatrix}$$

Now $51 = 8 \cdot 6 + 3$, so we add -6 times row 2 to row 1, getting:

$$\begin{bmatrix} 3 & 43 & -221 \\ 8 & -7 & 36 \end{bmatrix}$$

Now $8 = 3 \cdot 2 + 2$, so we add -2 times row 1 to row 2, getting:

$$\begin{bmatrix} 3 & 43 & -221 \\ 2 & -93 & 478 \end{bmatrix}$$

Then $3 = 2 \cdot 1 + 1$, so we add -1 times row 2 to row 1, getting:

$$\begin{bmatrix} 1 & 136 & -699 \\ 2 & -93 & 478 \end{bmatrix}$$

Finally, $2 = 1 \cdot 2$ so if we add -2 times row 1 to row 2 we get:

$$(*) \qquad \begin{bmatrix} 1 & 136 & -699 \\ 0 & -365 & 1876 \end{bmatrix}.$$

This tells us that

$$\boxed{\gcd(1876, 365) = 1}$$

and

$$(**) \qquad \boxed{1 = 136 \cdot 1876 + (-699)365.}$$

Note that it was not necessary to compute the last two entries -365 and 1876 in $(*)$. It is a good idea however to check that equation $(**)$ holds. In this case we have:

$$\begin{aligned} 136 \cdot 1876 &= 255136 \\ \underline{(-699) \cdot 365} &= \underline{-255135} \\ &1 \end{aligned}$$

So it is correct.

Why Blankinship's Method works: Note that just looking at what happens in the first column you see that we are just doing the Euclidean Algorithm, so when one element in column 1 is 0, the other is, in fact, the gcd. Note that at the start we have

$$\begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$$

and

$$\begin{aligned} a &= 1 \cdot a + 0 \cdot b \\ b &= 0 \cdot a + 1 \cdot b. \end{aligned}$$

One can show that at *every* intermediate step

$$\begin{bmatrix} a_1 & x_1 & x_2 \\ b_1 & y_1 & y_2 \end{bmatrix}$$

we always have

$$\begin{aligned} a_1 &= x_1 a + x_2 b \\ b_1 &= y_1 a + y_2 b, \end{aligned}$$

and the result follows. I will omit the details.

Exercise 9.1. Use Blankinship's method to compute the s and t in Bezout's Lemma for each of the following values of a and b.

(1) $a = 267$, $b = 112$

(2) $a = 216$, $b = 135$

(3) $a = 11312$, $b = 11321$

Exercise 9.2. Show that if $1 = as + bt$ then $\gcd(a, b) = 1$.

Exercise 9.3. Find integers a, b, d, s, t such that all of the following hold

(1) $a > 0$, $b > 0$,

(2) $d = sa + tb$, and

(3) $d \neq \gcd(a, b)$.

Note that d in Exercise 9.3 cannot be 1 by Exercise 9.2.

Chapter 10

Prime Numbers

Definition 10.1. An integer p is **prime** if $p \geq 2$ and the only positive divisors of p are 1 and p. An integer n is **composite** if $n \geq 2$ and n is not prime.

Remark 10.1. The number 1 is neither prime nor composite.

Lemma 10.1. *An integer $n \geq 2$ is composite if and only if there are integers a and b such that $n = ab$, $1 < a < n$, and $1 < b < n$.*

Proof. Let $n \geq 2$. If n is composite there is a positive integer a such that $a \neq 1$, $a \neq n$ and $a \mid n$. This means that $n = ab$ for some b. Since n and a are positive so is b. Hence $1 \leq a$ and $1 \leq b$. By Theorem 3.1(10) $a \leq n$ and $b \leq n$. Since $a \neq 1$ and $a \neq n$ we have $1 < a < n$. If $b = 1$ then $a = n$, which is not possible, so $b \neq 1$. If $b = n$ then $a = 1$, which is also not possible. So $1 < b < n$. The converse is obvious. $\square$

Lemma 10.2. *If $n > 1$, there is a prime p such that $p \mid n$.*

Proof. Assume there is some integer $n > 1$ which has no prime divisor. Let S denote the set of all such integers. By the Well-Ordering Property there is a smallest such integer, call it m. Now $m > 1$ and has no prime divisor. So m cannot be prime. Hence m is composite. Therefore by Lemma 10.1

$$m = ab, \quad 1 < a < m, \quad 1 < b < m.$$

Since $1 < a < m$ then a is not in the set S. So a must have a prime divisor, call it p. Then $p \mid a$ and $a \mid m$ so by Theorem 3.1, $p \mid m$. This contradicts the fact that m has no prime divisor. So the set S must be empty and this proves the lemma. $\square$

Theorem 10.1 (Euclid's Theorem). *There are infinitely many prime numbers.*

Proof. Assume, by way of contradiction, that there are only a finite number of prime numbers, say:

$$p_1, p_2, \ldots, p_n.$$

Define

$$N = p_1 p_2 \cdots p_n + 1.$$

Since $p_1 \geq 2$, clearly $N \geq 3$. So by Lemma 10.2 N has a prime divisor p. By assumption $p = p_i$ for some $i = 1, \ldots, n$. Let $a = p_1 \cdots p_n$. Note that

$$a = p_i \left(p_1 p_2 \cdots p_{i-1} p_{i+1} \cdots p_n\right),$$

so $p_i \mid a$. Now $N = a + 1$ and by assumption $p_i \mid a + 1$. So by Exercise 3.2 $p_i \mid (a+1) - a$, that is $p_i \mid 1$. By Basic Axiom 3 in Chapter 1 this implies that $p_i = 1$. This contradicts the fact that primes are > 1. It follows that the assumption that there are only finitely many primes is not true. $\square$

Exercise 10.1. Use the idea of the above proof to show that if $q_1, q_2, \ldots, q_n$ are primes there is a prime $q \notin \{q_1, \ldots, q_n\}$. Hint: Take $N = q_1 \cdots q_n + 1$. By Lemma 10.2 there is a prime q such that $q \mid N$. Prove that $q \notin \{q_1, \ldots, q_n\}$.

Exercise 10.2. Let $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$ and, in general, $p_i =$ the i-th prime. Prove or disprove that

$$p_1 p_2 \cdots p_n + 1$$

is prime for all $n \geq 1$. *[Hint: If $n = 1$ we have $2 + 1 = 3$ is prime. If $n = 2$ we have $2 \cdot 3 + 1 = 7$ is prime. If $n = 3$ we have $2 \cdot 3 \cdot 5 + 1 = 31$ is prime. Try the next few values of n. You may want to use the next theorem to check primality.]*

Theorem 10.2. *If $n > 1$ is composite then n has a prime divisor $p \leq \sqrt{n}$.*

Proof. Let $n > 1$ be composite. Then $n = ab$ where $1 < a < n$ and $1 < b < n$. I claim that one of a or b is $\leq \sqrt{n}$. If not then $a > \sqrt{n}$ and $b > \sqrt{n}$. Hence $n = ab > \sqrt{n}\sqrt{n} = n$. This implies $n > n$, a contradiction. So $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. Suppose $a \leq \sqrt{n}$. Since $1 < a$, by Lemma 10.2 there is a prime p such that $p \mid a$. Hence, by Theorem 3.1 since $a \mid n$ we have $p \mid n$. Also by Theorem 3.1 since $p \mid a$ we have $p \leq a \leq \sqrt{n}$. $\square$

Remark 10.2. We can use Theorem 10.2 to help decide whether or not an integer is prime: To check whether or not $n > 1$ is prime we need only try to divide it by all primes $p \leq \sqrt{n}$. If none of these primes divides n then n must be prime.

Example 10.1. Consider the number 97. Note that $\sqrt{97} < \sqrt{100} = 10$. The primes ≤ 10 are 2, 3, 5, and 7. One easily checks that $97 \bmod 2 = 1$, $97 \bmod 3 = 1$, $97 \bmod 5 = 2$, $97 \bmod 7 = 6$. So none of the primes 2, 3, 5, 7 divide 97 and 97 is prime by Theorem 10.2.

Exercise 10.3. By using Theorem 10.2, as in the above example, determine the primality[1] of the following integers:

$$143, \quad 221, \quad 199, \quad 223, \quad 3521.$$

Definition 10.2. Let $x \in \mathbb{R}$, $x > 0$. $\pi(x)$ denotes the number of primes p such that $p \leq x$.

For example, since the only primes $p \leq 10$ are 2, 3, 5, and 7 we have $\pi(10) = 4$.

Here is a table of values of $\pi(10^i)$ for $i = 2, \ldots, 10$. I also include known approximations to $\pi(x)$. Note that the formulas for the approximations do not give integer values, but for the table I have rounded each to the nearest integer. The values in the table were computed using Maple.

x	$\pi(x)$	$\frac{x}{ln(x)}$	$\frac{x}{ln(x)-1}$	$\int_2^x \frac{1}{ln(t)}dt$
10^2	25	22	28	29
10^3	168	145	169	177
10^4	1229	1086	1218	1245
10^5	9592	8686	9512	9629
10^6	78498	72382	78030	78627
10^7	664579	620421	661459	664917
10^8	5761455	5428681	5740304	5762208
10^9	50847534	48254942	50701542	50849234
10^{10}	455052511	434294482	454011971	455055614

You may judge for yourself which approximations appear to be the best. This table has been continued up to 10^{21}, but people are still working on finding

[1] This means determine whether or not each number is prime.

the value of $\pi(10^{22})$. Of course, the approximations are easy to compute with Maple but the exact value of $\pi(10^{22})$ is difficult to find.

The above approximations are based on the so-called *Prime Number Theorem* first conjectured by Gauss in 1793 but not proved till over 100 years later by Hadamard and Vallée Poussin.

Theorem 10.3 (The Prime Number Theorem).

$$(*) \qquad \pi(x) \sim \frac{x}{\ln(x)} \qquad \textit{for all } x > 0.$$

Remark 10.3. $(*)$ means that

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln(x)}} = 1.$$

Although there are infinitely many primes there are long stretches of consecutive integers containing no primes.

Theorem 10.4. *For any positive integer n there is an integer a such that the n consecutive integers*

$$a, a+1, a+2, \ldots, a+(n-1)$$

are all composite.

Proof. Given $n \geq 1$ let $a = (n+1)! + 2$. We claim that all the numbers

$$a + i, \quad 0 \leq i \leq n-1$$

are composite. Since $(n+1) \geq 2$ clearly $2 \mid (n+1)!$ and $2 \mid 2$. Hence $2 \mid (n+1)! + 2$. Since $(n+1)! + 2 > 2$, $(n+1)! + 2$ is composite. Consider

$$a + i = (n+1)! + i + 2$$

where $0 \leq i \leq n-1$ so $2 \leq i+2 \leq n+1$. Thus $i+2 \mid (n+1)!$ and $i+2 \mid i+2$. Therefore $i+2 \mid a+i$. Now $a+i > i+2 > 1$, so $a+i$ is composite. □

Exercise 10.4. Use the Prime Number Theorem and a calculator to approximate the number of primes $\leq 10^8$. Note $\ln(10^8) = 8\ln(10)$.

Exercise 10.5. Find 10 consecutive composite numbers.

Exercise 10.6. Prove that 2 is the only even prime number. (Joke: Hence it is said that 2 is the "oddest" prime.)

Exercise 10.7. Prove that if a and n are positive integers such that $n \geq 2$ and $a^n - 1$ is prime then a must be 2. *[Hint: By Exercise* 2.4

$$1 + x + x^2 + \cdots + x^{n-1} = \frac{(x^n - 1)}{x - 1}$$

that is,

$$x^n - 1 = (x - 1)\left(1 + x + x^2 + \cdots + x^{n-1}\right)$$

if $x \neq 1$ *and* $n \geq 1$.*]*

Exercise 10.8. (a) Is $2^n - 1$ always prime if $n \geq 2$? Explain. (b) Is $2^n - 1$ always prime if n is prime? Explain.

Exercise 10.9. Show that if p and q are primes and $p \mid q$, then $p = q$.

Chapter 11

Unique Factorization

Our goal in this chapter is to prove the following fundamental theorem.

Theorem 11.1 (The Fundamental Theorem of Arithmetic). *Every integer $n > 1$ can be written uniquely in the form*

$$n = p_1 p_2 \cdots p_s,$$

where s is a positive integer and $p_1, p_2, \ldots, p_s$ are primes satisfying

$$p_1 \leq p_2 \leq \cdots \leq p_s.$$

Remark 11.1. If $n = p_1 p_2 \cdots p_s$ where each p_i is prime, we call this the **prime factorization** of n. Theorem 11.1 is sometimes stated as follows:

> Every integer $n > 1$ can be expressed as a product $n = p_1 p_2 \cdots p_s$, for some positive integer s, where each p_i is prime and this factorization is unique except for the order of the primes p_i.

Note for example that

$$\begin{aligned} 600 &= 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \\ &= 2 \cdot 3 \cdot 2 \cdot 5 \cdot 2 \cdot 5 \\ &= 3 \cdot 5 \cdot 2 \cdot 2 \cdot 2 \cdot 5 \\ &\ \ \text{etc.} \end{aligned}$$

Perhaps the nicest way to write the prime factorization of 600 is

$$600 = 2^3 \cdot 3 \cdot 5^2.$$

In general it is clear that $n > 1$ can be written uniquely in the form

$$\boxed{(*) \qquad n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}, \text{ some } s \geq 1,}$$

where $p_1 < p_2 < \cdots < p_s$ and $a_i \geq 1$ for all i. Sometimes $(*)$ is written

$$\boxed{n = \prod_{i=1}^{s} p_i^{a_i}}.$$

Here $\prod$ stands for product, just as $\sum$ stands for sum.

To prove Theorem 11.1 we need to first establish a few lemmas.

Lemma 11.1. *If* $a \mid bc$ *and* $\gcd(a, b) = 1$ *then* $a \mid c$.

Proof. Since $\gcd(a, b) = 1$ by Bezout's Lemma there are s, t such that

$$1 = as + bt.$$

If we multiply both sides by c we get

$$c = cas + cbt = a(cs) + (bc)t.$$

By assumption $a \mid bc$. Clearly $a \mid a(cs)$ so, by Theorem 3.1, a divides the linear combination $a(cs) + (bc)t = c$. □

Definition 11.1. We say that a and b are *relatively prime* if $\gcd(a, b) = 1$.

So we may restate Lemma 11.1 as follows: *If* $a \mid bc$ *and* a *is relatively prime to* b *then* $a \mid c$.

Example 11.1. It is not true generally that when $a \mid bc$ then $a \mid b$ or $a \mid c$. For example, $6 \mid 4 \cdot 9$, but $6 \nmid 4$ and $6 \nmid 9$. Note that Lemma 11.1 doesn't apply here since $\gcd(6, 4) \neq 1$ and $\gcd(6, 9) \neq 1$.

Lemma 11.2 (Euclid's Lemma). *If* p *is a prime and* $p \mid ab$*, then* $p \mid a$ *or* $p \mid b$.

Proof. Assume that $p \mid ab$. If $p \mid a$ we are done. Suppose $p \nmid a$. Let $d = \gcd(p, a)$. Note that $d > 0$ and $d \mid p$ and $d \mid a$. Since $d \mid p$ we have $d = 1$ or $d = p$. If $d \neq 1$ then $d = p$. But this says that $p \mid a$, which we assumed was not true. So we must have $d = 1$. Hence $\gcd(p, a) = 1$ and $p \mid ab$. So by Lemma 11.1, $p \mid b$. □

Lemma 11.3. *Let p be prime. Let $a_1, a_2, \ldots, a_n$, $n \geq 1$, be integers. If $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_i$ for at least one $i \in \{1, 2, \ldots, n\}$.*

Proof. We use induction on n. The result is clear if $n = 1$. Assume that the lemma holds for n such that $1 \leq n \leq k$. Let's show it holds for $n = k+1$. So assume p is a prime and $p \mid a_1 a_2 \cdots a_k a_{k+1}$. Let $a = a_1 a_2 \cdots a_k$ and $b = a_{k+1}$. Then $p \mid a$ or $p \mid b$ by Lemma 11.2. If $p \mid a = a_1 \cdots a_k$, by the induction hypothesis, $p \mid a_i$ for some $i \in \{1, \ldots, k\}$. If $p \mid b = a_{k+1}$ then $p \mid a_{k+1}$. So we can say $p \mid a_i$ for some $i \in \{1, 2, \ldots, k+1\}$. So the lemma holds for $n = k+1$. Hence by PMI it holds for all $n \geq 1$. $\square$

Lemma 11.4 (Existence Part of Theorem 11.1). *If $n > 1$ then there exist primes $p_1, \ldots, p_s$ for some $s \geq 1$ such that*

$$n = p_1 p_2 \cdots p_s$$

and $p_1 \leq p_2 \leq \cdots \leq p_s$.

Proof. Proof by induction on n, with starting value $n = 2$: If $n = 2$ then since 2 is prime we can take $p_1 = 2$, $s = 1$. Assume the lemma holds for n such that $2 \leq n \leq k$. Let's show it holds for $n = k+1$. If $k+1$ is prime we can take $s = 1$ and $p_1 = k+1$ and we are done. If $k+1$ is composite we can write $k+1 = ab$ where $1 < a < k+1$ and $1 < b < k+1$. By the induction hypothesis there are primes $p_1, \ldots, p_u$ and $q_1, \ldots, q_v$ such that

$$a = p_1 \cdots p_u \text{ and } b = q_1 \cdots q_v.$$

This gives us

$$k+1 = ab = p_1 p_2 \cdots p_u q_1 q_2 \cdots q_v,$$

that is $k+1$ is a product of primes. Let $s = u+v$. By reordering and relabeling where necessary we have

$$k+1 = p_1 p_2 \cdots p_s$$

where $p_1 \leq p_2 \leq \cdots \leq p_s$. So the lemma holds for $n = k+1$. Hence by PMI, it holds for all $n > 1$. $\square$

Lemma 11.5 (Uniqueness Part of Theorem 11.1). *Let*

$$n = p_1 p_2 \cdots p_s \textit{ for some } s \geq 1,$$

and

$$n = q_1 q_2 \cdots q_t \text{ for some } t \geq 1,$$

where $p_1, \ldots, p_s, q_1, \ldots, q_t$ *are primes satisfying*

$$p_1 \leq p_2 \leq \cdots \leq p_s$$

and

$$q_1 \leq q_2 \leq \cdots \leq q_t.$$

Then, $t = s$ *and* $p_i = q_i$ *for* $i = 1, 2, \ldots, t$.

Proof. Our proof is by induction on s. Suppose $s = 1$. Then $n = p_1$ is prime and we have

$$p_1 = n = q_1 q_2 \cdots q_t.$$

If $t > 1$, this contradicts the fact that p_1 is prime. So $t = 1$ and we have $p_1 = q_1$, as desired. Now assume the result holds for all s such that $1 \leq s \leq k$. We want to show that it holds for $s = k + 1$. So assume

$$n = p_1 p_2 \cdots p_k p_{k+1}$$

and

$$n = q_1 q_2 \cdots q_t$$

where $p_1 \leq p_2 \leq \cdots \leq p_{k+1}$ and $q_1 \leq q_2 \leq \cdots \leq q_t$. Clearly $p_{k+1} \mid n$ so $p_{k+1} \mid q_1 \cdots q_t$. So by Lemma 11.3 $p_{k+1} \mid q_i$ for some $i \in \{1, 2, \ldots, t\}$. It follows from Exercise 10.9 that $p_{k+1} = q_i$. Hence $p_{k+1} = q_i \leq q_t$.

By a similar argument $q_t \mid n$ so $q_t \mid p_1 \cdots p_{k+1}$ and $q_t = p_j$ for some j. Hence $q_t = p_j \leq p_{k+1}$. This shows that

$$p_{k+1} \leq q_t \leq p_{k+1}$$

so $p_{k+1} = q_t$. Note that

$$p_1 p_2 \cdots p_k p_{k+1} = q_1 q_2 \cdots q_{t-1} q_t$$

Since $p_{k+1} = q_t$ we can cancel this prime from both sides and we have

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_{t-1}.$$

Now by the induction hypothesis $k = t - 1$ and $p_i = q_i$ for $i = 1, \ldots, t - 1$. Thus we have $k + 1 = t$ and $p_i = q_i$ for $i = 1, 2, \ldots, t$. So the lemma holds for $s = k + 1$ and by the PMI, it holds for all $s \geq 1$. $\square$

Now the proof of Theorem 11.1 follows immediately from Lemmas 11.4 and 11.5.

Remark 11.2. If a and b are positive integers we can find primes $p_1, \ldots, p_k$ and integers $a_1, \ldots, a_k, b_1, \ldots, b_k$ each ≥ 0 such that

$$(**) \qquad \begin{cases} a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \\ b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k} \end{cases}$$

For example, if $a = 600$ and $b = 252$ we have

$$\begin{aligned} 600 &= 2^3 \cdot 3^1 \cdot 5^2 \cdot 7^0 \\ 252 &= 2^2 \cdot 3^2 \cdot 5^0 \cdot 7. \end{aligned}$$

It follows that

$$\gcd(600, 252) = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^0.$$

In general, if a and b are given by $(**)$ we have

$$\boxed{\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_k^{\min(a_k, b_k)}}.$$

This gives one way to calculate the gcd *provided* you can factor both numbers. But generally speaking factorization is *very difficult*! On the other hand, the Euclidean algorithm is relatively fast.

Exercise 11.1. Find the prime factorizations of 1147 and 1716 by trying all primes $p \leq \sqrt{1147}$ ($p \leq \sqrt{1716}$) in succession.

Chapter 12

Fermat Primes and Mersenne Primes

Finding large primes and proving that they are indeed prime is not easy. One way to find large primes is to look at numbers that have some special form, for example, numbers of the form $a^n + 1$ or $a^n - 1$. It is easy to rule out some values of a and n. For example we have:

Theorem 12.1. *Let $a > 1$ and $n > 1$. Then*

(1) *$a^n - 1$ is prime $\Rightarrow a = 2$ and n is prime*

(2) *$a^n + 1$ is prime $\Rightarrow a$ is even and $n = 2^k$ for some $k \geq 1$.*

Proof of (1). We know from Exercise 2.5, page 6, that

$$\boxed{(*) \qquad a^n - 1 = (a-1)(a^{n-1} + \cdots + a + 1)}$$

Note that if $a > 2$ and $n > 1$ then $a - 1 > 1$ and $a^{n-1} + \cdots + a + 1 > a + 1 > 3$ so both factors in $(*)$ are > 1 and $a^n - 1$ is not prime. Hence if $a^n - 1$ is prime we must have $a = 2$. Now suppose $2^n - 1$ is prime. We claim that n is prime. If not $n = st$ where $1 < s < n$, $1 < t < n$. Then

$$2^n - 1 = 2^{st} - 1 = (2^s)^t - 1$$

is prime. But we just showed that if $a^n - 1$ is prime we must have $a = 2$. So we must have $2^s = 2$. Hence $s = 1$, $t = n$. So n is not composite. Hence n must be prime. This proves (1). □

Proof of (2). From ($*$) on p. 43 we have

$$(*) \qquad a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1).$$

Replace a by $-a$ in ($*$) and we get

$$(**) \qquad (-a)^n - 1 = (-a-1)\left((-a)^{n-1} + (-a)^{n-2} + \cdots + (-a) + 1\right)$$

Since n is odd, $n-1$ is even, $n-2$ is odd, ..., etc., we have $(-a)^n = -a^n, (-a)^{n-1} = a^{n-1}, (-a)^{n-2} = -a^{n-2}, \ldots$, etc. So ($**$) yields

$$-(a^n + 1) = -(a+1)\left(a^{n-1} - a^{n-2} + \cdots + -a + 1\right).$$

Multiplying both sides by -1 we get

$$(a^n + 1) = (a+1)(a^{n-1} - a^{n-2} + \cdots - a + 1)$$

when n is odd. If $n \geq 2$ we have $1 < a+1 < a^n + 1$. This shows that if n is odd and $a > 1$, $a^n + 1$ is not prime. Suppose $n = 2^s t$ where t is odd. Then if $a^n + 1$ is prime we have $(a^{2^s})^t + 1$ is prime. But by what we just showed this cannot be prime if t is odd and $t \geq 2$. So we must have $t = 1$ and $n = 2^s$. Also $a^n + 1$ prime implies that a is even since if a is odd so is a^n. Then $a^n + 1$ would be even. The only even prime is 2. But since we assume $a > 1$ we have $a \geq 2$ so $a^n + 1 \geq 3$. ☐

Definition 12.1. A number of the form $M_n = 2^n - 1$, $n \geq 2$, is said to be a **Mersenne number**. If M_n is prime, it is called a **Mersenne prime**. A number of the form $F_n = 2^{(2^n)} + 1$, $n \geq 0$, is called a **Fermat number**. If F_n is prime, it is called a **Fermat prime**.

One may prove that $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ and $F_4 = 65537$ are primes. As n increases the numbers $F_n = 2^{(2^n)} + 1$ increase in size very rapidly, and are not easy to check for primality. It is known that F_n is composite for many values of $n \geq 5$. This includes all n such that $5 \leq n \leq 30$ and a large number of other values of n including 382447 (the largest one I know of). It is now conjectured that F_n is composite for $n \geq 5$. So Fermat's original thought that F_n is prime for $n \geq 0$ seems to be pretty far from reality.

Exercise 12.1. Use Maple to factor F_5. [Go to any campus computer lab. Click or double-click on the Maple icon—or ask the lab assistant where it is located. When the window comes up, type at the prompt > the following:

```
> ifactor(2^32 + 1);
```

Hit the return key and you will get the answer.]

$M_3 = 2^3 - 1 = 7$ is a Mersenne prime and $M_4 = 2^4 - 1 = 15$ is a Mersenne number which is not a prime. At first it was thought that $M_p = 2^p - 1$ is prime whenever p is prime. But $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$ is not prime.

Over the years people have continued to work on the problem of determining for which primes p, $M_p = 2^p - 1$ is prime. To date 39 Mersenne primes have been found. It is known that $2^p - 1$ is prime if p is one of the following 39 primes 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593, 13466917.

The largest one, $M_{13466917} = 2^{13466917} - 1$, was found on November 14, 2001. The decimal representation of this number has $4,053,946$ digits. It was found by the team of Michael Cameron, George Woltman, Scott Kurowski *et al*, as a part of the **Great Internet Mersenne Prime Search (GIMPS)**, see Chris Caldwell's page for more about this. This prime could be the 39th Mersenne prime (in order of size), but we will only know this for sure when GIMPS completes testing all exponents below this one.You can find the link to Chris Caldwell's page on the class syllabus on my homepage. Later we show the connection between Mersenne primes and **perfect numbers**.

Lemma 12.1. *If M_n is prime, then n is prime.*

Proof. This is immediate from Theorem 12.1 (1). □

The most basic question about Mersenne primes is: *Are there infinitely many Mersenne primes?*

Exercise 12.2. Determine which Mersenne numbers M_n are prime when $2 \leq n \leq 12$. You may use Maple for this exercise. The Maple command for determining whether or not an integer n is prime is

```
isprime(n);
```

The following primality test for Mersenne numbers makes it easier to check whether or not M_p is prime when p is a large prime.

Theorem 12.2 (The Lucas-Lehmer Mersenne Prime Test). *Let p be an* odd *prime. Define the sequence*

$$r_1, r_2, r_3, \ldots, r_{p-1}$$

by the rules

$$r_1 = 4$$

and for $k \geq 2$,

$$r_k = (r_{k-1}^2 - 2) \bmod M_p.$$

Then M_p is prime if and only if $r_{p-1} = 0$.

[The proof of this is not easy. One place to find a proof is the book "A Selection of Problems in the Theory of Numbers" by W. Sierpinski, Pergamon Press, 1964.]

Example 12.1. Let $p = 5$. Then $M_p = M_5 = 31$.

$$\begin{aligned}
r_1 &= 4 \\
r_2 &= (4^2 - 2) \bmod 31 = 14 \bmod 31 = 14 \\
r_3 &= (14^2 - 2) \bmod 31 = 194 \bmod 31 = 8 \\
r_4 &= (8^2 - 2) \bmod 31 = 62 \bmod 31 = 0.
\end{aligned}$$

Hence by the Lucas-Lehmer test, $M_5 = 31$ is prime.

Exercise 12.3. Show using the Lucas-Lehmer test that $M_7 = 127$ is prime.

Remark 12.1. Note that the Lucas-Lehmer test for $M_p = 2^p - 1$ takes only $p-1$ steps. On the other hand, if one attempts to prove M_p prime by testing all primes $\leq \sqrt{M_p}$ one must consider about $2^{\frac{p}{2}}$ steps. This is MUCH larger than p in general.

Chapter 13

The Functions σ and τ

Definition 13.1. For $n > 0$ define:

$$\begin{aligned}\tau(n) &= \text{the number of positive divisors of } n,\\ \sigma(n) &= \text{the sum of the positive divisors of } n.\end{aligned}$$

Example 13.1. $12 = 3 \cdot 2^2$ has positive divisors

$$1, 2, 3, 4, 6, 12.$$

Hence

$$\tau(12) = 6$$

and

$$\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28.$$

Definition 13.2. A positive divisor d of n is said to be a **proper divisor** of n if $d < n$. We denote the sum of all proper divisors of n by $\sigma^*(n)$.

Note that if $n \geq 2$ then

$$\sigma^*(n) = \sigma(n) - n.$$

Example 13.2. $\sigma^*(12) = 16$.

Definition 13.3. $n > 1$ is **perfect** if $\sigma^*(n) = n$.

Example 13.3. The proper divisors of 6 are 1, 2 and 3. So $\sigma^*(6) = 6$. Therefore 6 is perfect.

Exercise 13.1. Prove that 28 is perfect.

The next theorem shows a simple way to compute $\sigma(n)$ and $\tau(n)$ from the prime factorization of n.

Theorem 13.1. *Let*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}, \quad r \geq 1,$$

where $p_1 < p_2 < \cdots < p_r$ *are primes and* $e_i \geq 0$ *for each* $i \in \{1, 2, \ldots, r\}$. *Then*

(1) $\tau(n) = (e_1 + 1)(e_2 + 1) \cdots (e_r + 1)$

(2) $\sigma(n) = \left(\frac{p_1^{e_1+1} - 1}{p_1 - 1}\right)\left(\frac{p_2^{e_2+1} - 1}{p_2 - 1}\right) \cdots \left(\frac{p_r^{e_r+1} - 1}{p_r - 1}\right).$

Before proving this let's look at an example. Take $n = 72 = 8 \cdot 9 = 2^3 \cdot 3^2$. The theorem says

$$\begin{aligned} \tau(72) &= (3+1)(2+1) = 12 \\ \sigma(72) &= \left(\frac{2^4 - 1}{2 - 1}\right)\left(\frac{3^3 - 1}{3 - 1}\right) = 15 \cdot 13 = 195. \end{aligned}$$

[*Proof of Theorem* 13.1 *(1)*] From the Fundamental Theorem of Arithmetic every positive factor d of n will have its prime factors coming from those of n. Hence $d \mid n$ iff $d = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$ where for each i:

$$0 \leq f_i \leq e_i.$$

That is, for each f_i we can choose a value in the set of $e_i + 1$ numbers $\{0, 1, 2, \ldots, e_i\}$. So, in all, there are $(e_1 + 1)(e_2 + 1) \cdots (e_r + 1)$ choices for the exponents $f_1, f_2, \ldots, f_r$. So (1) holds.
[*Proof of (2)*] We first establish two lemmas.

Lemma 13.1. *Let* $n = ab$ *where* $a > 0$, $b > 0$ *and* $\gcd(a, b) = 1$. *Then* $\sigma(n) = \sigma(a)\sigma(b)$.

Proof. Since a and b have only 1 as a common factor, using the Fundamental Theorem of Arithmetic it is easy to see that $d \mid ab \Leftrightarrow d = d_1 d_2$ where $d_1 \mid a$

and $d_2 \mid b$. That is, the divisors of ab are products of the divisors of a and the divisors of b. Let

$$1, a_1, \ldots, a_s$$

denote the divisors of a and let

$$1, b_1, \ldots, b_t$$

denote the divisors of b. Then

$$\begin{aligned}\sigma(a) &= 1 + a_1 + a_2 + \cdots + a_s,\\ \sigma(b) &= 1 + b_1 + b_2 + \cdots + b_t.\end{aligned}$$

The divisors of $n = ab$ can be listed as follows

$$\begin{gathered}1, b_1, b_2, \ldots, b_t,\\ a_1 \cdot 1, a_1 \cdot b_1, a_1 \cdot b_2, \ldots, a_1 \cdot b_t,\\ a_2 \cdot 1, a_2 \cdot b_1, a_2 \cdot b_2, \ldots, a_2 \cdot b_t,\\ \vdots\\ a_s \cdot 1, a_s \cdot b_1, a_s \cdot b_2, \ldots, a_s \cdot b_t.\end{gathered}$$

It is important to note that since $gcd(a, b) = 1$, $a_i b_j = a_k b_\ell$ implies that $a_i = a_k$ and $b_j = b_\ell$. That is there are no repetitions in the above array.

If we sum each row we get

$$\begin{gathered}1 + b_1 + \cdots + b_t = \sigma(b)\\ a_1 1 + a_1 b_1 + \cdots + a_1 b_t = a_1 \sigma(b)\\ \vdots\\ a_s \cdot 1 + a_s b_1 + \cdots + a_s b_t = a_s \sigma(b).\end{gathered}$$

By adding these partial sums together we get

$$\begin{aligned}\sigma(n) &= \sigma(b) + a_1\sigma(b) + a_2\sigma(b) + \cdots + a_3\sigma(b)\\ &= (1 + a_1 + a_2 + \cdots + a_s)\sigma(b)\\ &= \sigma(a)\sigma(b).\end{aligned}$$

This proves the lemma. $\square$

Lemma 13.2. *If p is a prime and $k \geq 0$ we have*

$$\sigma(p^k) = \frac{p^{k+1}-1}{p-1}.$$

Proof. Since p is prime, the divisors of p^k are $1, p, p^2, \ldots, p^k$. Hence

$$\sigma(p^k) = 1 + p + p^2 + \cdots + p^k = \frac{p^{k+1}-1}{p-1},$$

as desired. $\square$

Proof of Theorem 13.1 *(2) (continued).* Let $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$. Our proof is by induction on r. If $r = 1$, $n = p_1^{e_1}$ and the result follows from Lemma 13.2. Suppose the result is true when $1 \leq r \leq k$. Consider now the case $r = k+1$. That is, let

$$n = p_1^{e_1} \cdots p_k^{e_k} p_{k+1}^{e_{k+1}}$$

where the primes $p_1, \ldots, p_k, p_{k+1}$ are distinct and $e_i \geq 0$. Let $a = p_1^{e_1} \cdots p_k^{e_k}$, $b = p_{k+1}^{e_{k+1}}$. Clearly $\gcd(a, b) = 1$. So by Lemma 13.1 we have $\sigma(n) = \sigma(a)\sigma(b)$. By the induction hypothesis

$$\sigma(a) = \left(\frac{p_1^{e_1+1}-1}{p_1-1}\right) \cdots \left(\frac{p_k^{e_k+1}-1}{p_k-1}\right)$$

and by Lemma 13.2

$$\sigma(b) = \frac{p_{k+1}^{e_{k+1}+1}-1}{p_{k+1}-1}$$

and it follows that

$$\sigma(n) = \left(\frac{p_1^{e_1+1}-1}{p_1-1}\right) \cdots \left(\frac{p_{k+1}^{e_{k+1}+1}-1}{p_{k+1}-1}\right).$$

So the result holds for $r = k+1$. By PMI it holds for $r \geq 1$. $\square$

Exercise 13.2. Find $\sigma(n)$ and $\tau(n)$ for the following values of n.

(1) $n = 900$

(2) $n = 496$

(3) $n = 32$

(4) $n = 128$

(5) $n = 1024$

Exercise 13.3. Determine which (if any) of the numbers in Exercise 13.2 are perfect.

Exercise 13.4. Does Lemma 13.1 hold if we replace σ by σ^*? *[Hint: The answer is no, but find explicit numbers a and b such that the result fails yet* $\gcd(a, b) = 1$.*]*

Chapter 14

Perfect Numbers and Mersenne Primes

If you do a search for perfect numbers up to $10,000$ you will find only the following perfect numbers:

$$\begin{aligned} 6 &= 2 \cdot 3, \\ 28 &= 2^2 \cdot 7, \\ 496 &= 2^4 \cdot 31, \\ 8128 &= 2^6 \cdot 127. \end{aligned}$$

Note that $2^2 = 4$, $2^3 = 8$, $2^5 = 32$, $2^7 = 128$ so we have:

$$\begin{aligned} 6 &= 2 \cdot (2^2 - 1), \\ 28 &= 2^2 \cdot (2^3 - 1), \\ 496 &= 2^4 \cdot (2^5 - 1), \\ 8128 &= 2^6 \cdot (2^7 - 1). \end{aligned}$$

Note also that $2^2 - 1$, $2^3 - 1$, $2^5 - 1$, $2^7 - 1$ are Mersenne primes. One might conjecture that all perfect numbers follow this pattern. We discuss to what extent this is known to be true. We start with the following result.

Theorem 14.1. *If $2^p - 1$ is a Mersenne prime, then $2^{p-1} \cdot (2^p - 1)$ is perfect.*

Proof. Write $q = 2^p - 1$ and let $n = 2^{p-1}q$. Since q is odd and prime, by Theorem 13.1 (2) we have $\sigma(n) = \sigma\left(2^{p-1}q\right) = \left(\frac{2^p-1}{2-1}\right)\left(\frac{q^2-1}{q-1}\right) = (2^p - 1)(q + 1) = (2^p - 1)2^p = 2n$. That is, $\sigma(n) = 2n$ and n is perfect. $\square$

Now we show that all *even* perfect numbers have the conjectured form.

Theorem 14.2. *If n is even and perfect then there is a Mersenne prime $2^p - 1$ such that $n = 2^{p-1}(2^p - 1)$.*

Proof. Let n be even and perfect. Since n is even, $n = 2m$ for some m. We take out as many powers of 2 as possible obtaining

$$(*) \qquad n = 2^k \cdot q, \quad k \geq 1,\ q \text{ odd}.$$

Since n is perfect $\sigma^*(n) = n$, that is, $\sigma(n) = 2n$. Since q is odd, $\gcd(2^k, q) = 1$, so by Lemmas 13.1 and 13.2:

$$\sigma(n) = \sigma(2^k)\sigma(q) = (2^{k+1} - 1)\sigma(q).$$

So we have

$$2^{k+1}q = 2n = \sigma(n) = (2^{k+1} - 1)\sigma(q),$$

hence

$$(**) \qquad 2^{k+1}q = (2^{k+1} - 1)\sigma(q).$$

Now $\sigma^*(q) = \sigma(q) - q$, so

$$\sigma(q) = \sigma^*(q) + q.$$

Putting this in $(**)$ we get

$$2^{k+1}q = (2^{k+1} - 1)(\sigma^*(q) + q)$$

or

$$2^{k+1}q = (2^{k+1} - 1)\sigma^*(q) + 2^{k+1}q - q$$

which implies

$$(***) \qquad \sigma^*(q)(2^{k+1} - 1) = q.$$

In other words, $\sigma^*(q)$ is a divisor of q. Since $k \geq 1$ we have $2^{k+1} - 1 \geq 4 - 1 = 3$. So $\sigma^*(q)$ is a proper divisor of q. But $\sigma^*(q)$ is the sum of *all* proper divisors of q. This can only happen if q has only one proper divisor. This means that q must be prime and $\sigma^*(q) = 1$. Then $(***)$ shows that $q = 2^{k+1} - 1$. So q must be a Mersenne prime and $k + 1 = p$ is prime. So $n = 2^{p-1} \cdot (2^p - 1)$, as desired. □

Corollary 14.1. *There is a* 1–1 *correspondence between* even *perfect numbers and Mersenne primes.*

Three Open Questions:

1. Are there infinitely many even perfect numbers?
2. Are there infinitely many Mersenne primes?
3. Are there any odd perfect numbers?

So far no one has found a single odd perfect number. It is known that if an odd perfect number exists, it must be $> 10^{50}$.

Remark 14.1. Some think that Euclid's knowledge that $2^{p-1}(2^p-1)$ is perfect when 2^p-1 is prime may have been his motivation for defining prime numbers.

Chapter 15

Congruences

Definition 15.1. Let $m \geq 0$. We write $a \equiv b \pmod{m}$ if $m \mid a - b$, and we say that a is *congruent* to b *modulo* m. Here m is said to be the *modulus of the congruence*. The notation $a \not\equiv b \pmod{m}$ means that it is false that $a \equiv b \pmod{m}$.

Examples 15.1.

(1) $25 \equiv 1 \pmod{4}$ since $4 \mid 24$

(2) $25 \not\equiv 2 \pmod{4}$ since $4 \nmid 23$

(3) $1 \equiv -3 \pmod{4}$ since $4 \mid 4$

(4) $a \equiv b \pmod{1}$ for all a, b since "1 divides everything."

(5) $a \equiv b \pmod{0} \iff a = b$ for all a, b since "0 divides only 0."

Remark 15.1. As you see, the cases $m = 1$ and $m = 0$ are not very interesting so mostly we will only be interested in the case $m \geq 2$.

WARNING. Do not confuse the use of mod in Definition 15.1 with that of Definition 5.3. We shall see that the two uses of mod are related, but have different meanings: Recall

$a \bmod b = r$ where r is the remainder given by the Division Algorithm when a is divided by b

and by Definition 15.1

$$\boxed{a \equiv b \pmod{m} \text{ means } m \mid a - b.}$$

Example 15.2.

$$\boxed{25 \equiv 5 \pmod{4} \text{ is true}},$$

since $4 \mid 20$ but

$$\boxed{25 = 5 \bmod 4 \text{ is false}},$$

since the latter means $25 = 1$.

Remark 15.2. The mod in $a \equiv b \pmod{m}$ defines a **binary relation**, whereas the mod in $a \bmod b$ is a **binary operation**.

More terminology: Expressions such as

$$x = 2$$
$$4^2 = 16$$
$$x^2 + 2x = \sin(x) + 3$$

are called **equations**. By analogy, expressions such as

$$x \equiv 2 \pmod{16}$$
$$25 \equiv 5 \pmod{5}$$
$$x^3 + 2x \equiv 6x^2 + 3 \pmod{27}$$

are called **congruences**. Before discussing further the analogy between equations and congruences, we show the relationship between the two different definitions of mod.

Theorem 15.1. *For $m > 0$ and for all a, b:*

$$a \equiv b \pmod{m} \iff a \bmod m = b \bmod m.$$

Proof. "$\Rightarrow$" Assume that $a \equiv b \pmod{m}$. Let $r_1 = a \bmod m$ and $r_2 = b \bmod m$. We want to show that $r_1 = r_2$. By definition we have

(1) $m \mid a - b$,

(2) $a = mq_1 + r_1$, $0 \leq r_1 < m$, and

(3) $b = mq_2 + r_2$, $0 \le r_2 < m$

From (1) we obtain
$$a - b = mt$$
for some t. Hence
$$a = mt + b.$$
Using (2) and (3) we see that
$$a = mq_1 + r_1 = m\,(q_2 + t) + r_2.$$
Since $0 \le r_1 < m$ and $0 \le r_2 < m$ by the uniqueness part of the Division Algorithm we obtain $r_1 = r_2$, as desired.

" $\Leftarrow$" Assume that $a \bmod m = b \bmod m$. We must show that $a \equiv b \pmod{m}$. Let $r = a \bmod m = b \bmod m$, then by definition we have
$$a = mq_1 + r, \quad 0 \le r < m,$$
and
$$b = mq_2 + r, \quad 0 \le r < m.$$
Hence
$$a - b = m\,(q_1 - q_2)\,.$$
This shows that $m \mid a - b$ and hence $a \equiv b \pmod{m}$, as desired. □

Exercise 15.1. Prove that for all $m > 0$ and for all a:
$$a \equiv a \bmod m \pmod{m}.$$

Exercise 15.2. Using Definition 15.1 show that the following congruences are true
$$\begin{aligned} 385 &\equiv 322 \pmod{3} \\ -385 &\equiv -322 \pmod{3} \\ 1 &\equiv -17 \pmod{3} \\ 33 &\equiv 0 \pmod{3}. \end{aligned}$$

Exercise 15.3. Use Theorem 15.1 to show that the congruences in Exercise 15.2 are valid.

Exercise 15.4. (a) Show that a is even $\Leftrightarrow a \equiv 0 \pmod 2$ and a is odd $\Leftrightarrow a \equiv 1 \pmod 2$. (b) Show that a is even $\Leftrightarrow a \bmod 2 = 0$ and a is odd $\Leftrightarrow a \bmod 2 = 1$.

Exercise 15.5. Show that if $m > 0$ and a is any integer, there is a *unique* integer $r \in \{0, 1, 2, \ldots, m-1\}$ such that $a \equiv r \pmod m$.

Exercise 15.6. Find integers a and b such that $0 < a < 15$, $0 < b < 15$ and $ab \equiv 0 \pmod{15}$.

Exercise 15.7. Find integers a and b such that $1 < a < 15$, $1 < b < 15$, and $ab \equiv 1 \pmod{15}$.

Exercise 15.8. Show that if $d \mid m$ and $d > 0$, then

$$a \equiv b \pmod m \Rightarrow a \equiv b \pmod d.$$

The next two theorems show that congruences and equations share many similar properties.

Theorem 15.2 (Congruence is an equivalence relation). *For all a, b, c and $m > 0$ we have*

(1) $a \equiv a \pmod m$ [**reflexivity**]

(2) $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$ [**symmetry**]

(3) $a \equiv b \pmod m$ *and* $b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$ [**transitivity**]

Proof of (1). $a - a = 0 = 0 \cdot m$, so $m \mid a - a$. Hence $a \equiv a \pmod m$. □

Proof of (2). If $a \equiv b \pmod m$, then $m \mid a - b$. Hence $a - b = mq$. Hence $b - a = m(-q)$, so $m \mid b - a$. Hence $b \equiv a \pmod m$. □

Proof of (3). If $a \equiv b \pmod m$ and $b \equiv c \pmod m$ then $m \mid a - b$ and $m \mid b - c$. By the linearity property $m \mid (a - b) + (b - c)$. That is, $m \mid a - c$. Hence $a \equiv c \pmod m$. □

Recall that a **polynomial** is an expression of the form

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0.$$

Here we will assume that the coefficients $a_n, \ldots, a_0$ are integers and x also represents an integer variable. Here, of course, $n \geq 0$ and n is an integer.

Theorem 15.3. *If* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$, *then*

(1) $a \pm c \equiv b \pm d \pmod{m}$

(2) $ac \equiv bd \pmod{m}$

(3) $a^n \equiv b^n \pmod{m}$ *for all* $n \geq 1$

(4) $f(a) \equiv f(b) \pmod{m}$ *for all polynomials* $f(x)$ *with integer coefficients.*

Proof of (1). To prove (1) since $a - c = a + (-c)$, it suffices to prove only the "+ case." By assumption $m \mid a - b$ and $m \mid c - d$. By linearity, $m \mid (a - b) + (c - d)$, that is $m \mid (a + c) - (b + d)$. Hence

$$a + c \equiv b + d \pmod{m}.$$

□

Proof of (2). Since $m \mid a - b$ and $m \mid c - d$ by linearity

$$m \mid c(a - b) + b(c - d).$$

Now $c(a - b) + b(c - d) = ca - bd$, hence

$$m \mid ca - bd,$$

and so $ca \equiv bd \pmod{m}$, as desired. □

Proof of (3). We prove $a^n \equiv b^n \pmod{m}$ by induction on n. If $n = 1$, the result is true by our assumption that $a \equiv b \pmod{m}$. Assume it holds for $n = k$. Then we have $a^k \equiv b^k \pmod{m}$. This, together with $a \equiv b \pmod{m}$ using (2) above, gives $aa^k \equiv bb^k \pmod{m}$. Hence $a^{k+1} \equiv b^{k+1} \pmod{m}$. So it holds for all $n \geq 1$, by the PMI. □

Proof of (4). Let $f(x) = c_n x^n + \cdots + c_1 x + c_0$. We prove by induction on n that if $a \equiv b \pmod{m}$ then

$$c_n a^n + \cdots + c_0 \equiv c_n b^n + \cdots + c_0 \pmod{m}.$$

If $n = 0$ we have $c_0 \equiv c_0 \pmod{m}$ by Theorem 15.2 (1). Assume the result holds for $n = k$. Then we have

$$(*) \qquad c_k a^k + \cdots + c_1 a + c_0 \equiv c_k b^k + \cdots + c_1 b + c_0 \pmod{m}.$$

By part (3) above we have $a^{k+1} \equiv b^{k+1} \pmod{m}$. Since $c_{k+1} \equiv c_{k+1} \pmod{m}$ using (2) above we have

$$(**) \qquad c_{k+1}a^{k+1} \equiv c_{k+1}b^{k+1} \pmod{m}.$$

Now we can apply Theorem 15.3 (1) to $(*)$ and $(**)$ to obtain

$$c_{k+1}a^{k+1} + c_k a^k + \cdots + c_0 \equiv c_{k+1}b^{k+1} + c_k b^k + \cdots + c_0 \pmod{m}.$$

So by the PMI, the result holds for $n \geq 0$. □

Before continuing to develop properties of congruences, we give the following example to show one way that congruences can be useful.

Example 15.3. (This example was taken from [1] *Introduction to Analytic Number Theory,* by Tom Apostol.)

The first five Fermat numbers

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65,537$$

are primes. We show using congruences *without explicitly calculating* F_5 that $F_5 = 2^{32} + 1$ is divisible by 641 and is therefore not prime :

$$\begin{aligned} 2^2 &= 4 \\ 2^4 &= \left(2^2\right)^2 = 4^2 = 16 \\ 2^8 &= \left(2^4\right)^2 = 16^2 = 256 \\ 2^{16} &= \left(2^8\right)^2 = 256^2 = 65,536 \end{aligned}$$

$$65,536 \equiv 154 \pmod{641}.$$

So we have

$$2^{16} \equiv 154 \pmod{641}.$$

By Theorem 15.3 (3):

$$\left(2^{16}\right)^2 \equiv (154)^2 \pmod{641}.$$

That is,

$$2^{32} \equiv 23,716 \pmod{641}.$$

Since

$$23,716 \equiv 640 \pmod{641}$$

and

$$640 \equiv -1 \pmod{641}$$

we have

$$2^{32} \equiv -1 \pmod{641}$$

and hence

$$2^{32} + 1 \equiv 0 \pmod{641}.$$

So $641 \mid 2^{32}+1$, as claimed. Clearly $2^{32}+1 \neq 641$, so $2^{32}+1$ is composite. Of course, if you already did Exercise 12.1 (p. 44) you will already know that

$$2^{32} + 1 = 4,294,967,297 = (641) \cdot (6,700,417)$$

and that 641 and $6,700,417$ are indeed primes. Note that 641 is the 116^{th} prime, so if you used trial division you would have had to divide by 115 primes before reaching one that divides $2^{32} + 1$, and that assumes that you have a list of the first 116 primes.

Theorem 15.4. *If* $m > 0$ *and*

$$a \equiv r \pmod{m} \text{ where } 0 \leq r < m$$

then $a \bmod m = r$.

Exercise 15.9. Prove Theorem 15.4. [Hint: The Division Algorithm may be useful.]

Exercise 15.10. Find the value of each of the following (*without using Maple*!).

(1) $2^{32} \bmod 7$

(2) $10^{35} \bmod 7$

(3) $3^{35} \bmod 7$

[**Hint:** Use Theorem 15.4 and the ideas used in the example on page 62.]

Exercise 15.11. Let $\gcd(m_1, m_2) = 1$. Prove that

$$a \equiv b \pmod{m_1} \text{ and } a \equiv b \pmod{m_2} \tag{15.1}$$

if and only if

$$a \equiv b \pmod{m_1 m_2}. \tag{15.2}$$

[Hint. Use Lemma 11.1, page 38.]

Chapter 16

Divisibility Tests for 2, 3, 5, 9, 11

Recall from Definition 4.2 on page 14 that the decimal representation of the positive integer a is given by

$$a = a_{n-1}a_{n-2}\cdots a_1a_0 \tag{1}$$

when

$$a = a_{n-1}10^{n-1} + a_{n-2}10^{n-2} + \cdots + a_1 10 + a_0$$

and $0 \le a_i \le 9$ for $i = 0, 1, \ldots, n-1$.

Theorem 16.1. *Let the decimal representation of a be given by* (1)*, then*

(a) $a \bmod 2 = a_0 \bmod 2$,

(b) $a \bmod 5 = a_0 \bmod 5$,

(c) $a \bmod 3 = (a_{n-1} + \cdots + a_0) \bmod 3$,

(d) $a \bmod 9 = (a_{n-1} + \cdots + a_0) \bmod 9$,

(e) $a \bmod 11 = (a_0 - a_1 + a_2 - a_3 + \cdots) \bmod 11$.

Before proving this theorem, let's give some examples.

$$1457 \bmod 2 = 7 \bmod 2 = 1$$
$$1457 \bmod 5 = 7 \bmod 5 = 2$$

$$\begin{aligned} 1457 \bmod 3 = (1+4+5+7) \bmod 3 &= 17 \bmod 3 \\ &= 8 \bmod 3 = 2 \end{aligned}$$

$$\begin{aligned}1457 \bmod 9 &= (1+4+5+7) \bmod 9\\ &= 17 \bmod 9\\ &= 8 \bmod 9\\ &= 8\end{aligned}$$

$$\begin{aligned}1457 \bmod 11 &= 7-5+4-1 \bmod 11\\ &= 5 \bmod 11\\ &= 5.\end{aligned}$$

Proof of Theorem 16.1. Consider the polynomial

$$f(x) = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Note that $10 \equiv 0 \pmod 2$. So by Theorem 15.3 (4)

$$a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0 \equiv a_{n-1}0^{n-1} + \cdots + a_1 0 + a_0 \pmod 2.$$

That is,

$$a \equiv a_0 \pmod 2.$$

This, together with Theorem 15.1, proves part (a). Since $10 \equiv 0 \pmod 5$, the proof of part (b) is similar.

Note that $10 \equiv 1 \pmod 3$ so applying theorem 15.3 (4) again, we have

$$a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0 \equiv a_{n-1}1^{n-1} + \cdots + a_1 1 + a_0 \pmod 3.$$

That is,

$$a \equiv a_{n-1} + \cdots + a_1 + a_0 \pmod 3.$$

This using Theorem 15.1 proves part (c). Since $10 \equiv 1 \pmod 9$, the proof of part (d) is similar.

Now $10 \equiv -1 \pmod{11}$ so

$$a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0 \equiv a_{n-1}(-1)^{n-1} + \cdots + a_1(-1) + a_0 \pmod{11}.$$

That is,

$$a \equiv a_0 - a_1 + a_2 - \cdots \pmod{11}$$

and by Theorem 15.1 we are done. $\square$

Remark 16.1. Note that

$$m \mid a \Leftrightarrow a \bmod m = 0,$$

so from Theorem 16.1 we obtain immediately the following corollary.

Corollary 16.1. *Let* a *be given by* (1), *p.* 65. *Then*

(a) $2 \mid a \Leftrightarrow a_0 = 0, 2, 4, 6$ *or* 8

(b) $5 \mid a \Leftrightarrow a_0 = 0$ *or* 5

(c) $3 \mid a \Leftrightarrow 3 \mid a_0 + a_1 + \cdots + a_{n-1}$

(d) $9 \mid a \Leftrightarrow 9 \mid a_0 + a_1 + \cdots + a_{n-1}$

(e) $11 \mid a \Leftrightarrow 11 \mid a_0 - a_1 + a_2 - a_3 + \cdots$.

Note that in applying (c), (d) and (e) we can use the fact that

$$(a + m) \bmod m = a$$

to "cast out" 3's (for (c)) and 9's (for (d)). Here's an example of "casting out 9's:"

$$\begin{aligned} 1487 \bmod 9 &= (1 + 4 + 8 + 7) \bmod 9 \\ &= (9 + 4 + 7) \bmod 9 \\ &= (4 + 7) \bmod 9 \\ &= (2 + 9) \bmod 9 \\ &= 2 \bmod 9 = 2. \end{aligned}$$

So $1487 \bmod 9 = 2$.

Note that if $0 \leq r < m$ then

$$r \bmod m = r.$$

Exercise 16.1. Let $a = 18726132117057$. Find $a \bmod m$ for $m = 2, 3, 5, 9$ and 11.

Exercise 16.2. Let $a = a_n \cdots a_1 a_0$ be the decimal representation of a. Then prove

(a) $a \bmod 10 = a_0$.

(b) $a \bmod 100 = a_1 a_0$.

(c) $a \bmod 1000 = a_2 a_1 a_0$.

Exercise 16.3. Prove that if b is a positive square, i.e., $b = a^2$, $a > 0$, then the least significant digit of b is one of 0, 1, 4, 5, 6, 9. [Hint: $b \bmod 10$ is the least significant digit of b. Write $a = a_{n-1} \cdots a_0$. Then $a \equiv a_0 \pmod{10}$ so $a^2 \equiv a_0^2 \pmod{10}$. For each digit $a_0 \in \{0, 1, 2, \ldots, 9\}$ find $a_0^2 \bmod 10$. Use Theorem 15.4, among other results.]

Exercise 16.4. Are any of the following numbers squares? Explain.

$$10, \quad 11, \quad 16, \quad 19, \quad 24, \quad 25, \quad 272, \quad 2983, \quad 11007, \quad 1120378$$

Chapter 17

Divisibility Tests for 7 and 13

Theorem 17.1. *Let $a = a_r a_{r-1} \cdots a_1 a_0$ be the decimal representation of a. Then*

(a) $7 \mid a \Leftrightarrow 7 \mid a_r \cdots a_1 - 2a_0$.

(b) $13 \mid a \Leftrightarrow 13 \mid a_r \cdots a_1 - 9a_0$.

[*Here* $a_r \cdots a_1 = \frac{a-a_0}{10} = a_r 10^{r-1} + \cdots + a_2 10 + a_1$.]

Before proving this theorem we illustrate it with two examples.

$$\begin{aligned} 7 \mid 2481 &\Leftrightarrow 7 \mid 248 - 2 \\ &\Leftrightarrow 7 \mid 246 \\ &\Leftrightarrow 7 \mid 24 - 12 \\ &\Leftrightarrow 7 \mid 12 \end{aligned}$$

since $7 \nmid 12$ we have $7 \nmid 2481$.

$$\begin{aligned} 13 \mid 12987 &\Leftrightarrow 13 \mid 1298 - 63 \\ &\Leftrightarrow 13 \mid 1235 \\ &\Leftrightarrow 13 \mid 123 - 45 \\ &\Leftrightarrow 13 \mid 78 \end{aligned}$$

since $6 \cdot 13 = 78$, we have $13 \mid 78$. So, by Theorem 17.1 (b), $13 \mid 12987$.

Proof of 17.1 (a). Let $c = a_r \cdots a_1$. So we have $a = 10c + a_0$. Hence $-2a = -20c - 2a_0$. Now $1 \equiv -20 \pmod 7$ so we have

$$-2a \equiv c - 2a_0 \pmod 7.$$

It follows from Theorem 15.1 that

$$-2a \bmod 7 = c - 2a_0 \bmod 7.$$

Hence, $7 \mid -2a \Leftrightarrow 7 \mid c - 2a_0$. Since $\gcd(7, -2) = 1$ we have $7 \mid -2a \Leftrightarrow 7 \mid a$. Hence $7 \mid a \Leftrightarrow 7 \mid c - 2a_0$, which is what we wanted to prove. □

Proof of 17.1 (b). (This has a similar proof to that for 17.1 (a) and is left for the interested reader.) □

Exercise 17.1. Use Theorem 17.1 (a) to determine which of the following are divisible by 7:

(a) 6994 (b) 6993

Exercise 17.2. In the notation of Theorem 17.1, show that $a \bmod 7$ need not be equal to $(a_r \cdots a_1 - 2a_0) \bmod 7$..

Chapter 18

More Properties of Congruences

Theorem 18.1. *Let $m \geq 2$. If a and m are relatively prime, there exists a unique integer a^* such that $aa^* \equiv 1 \pmod{m}$ and $0 < a^* < m$.*

We call a^* the *inverse of a* **modulo** m. Note that we do not denote a^* by a^{-1} since this might cause some confusion. Of course, if $c \equiv a^* \pmod{m}$ then $ac \equiv 1 \pmod{m}$ so a^* is not unique unless we specify that $0 < a^* < m$.

Proof. If $\gcd(a, m) = 1$, then by Bezout's Lemma there exist s and t such that

$$as + mt = 1.$$

Hence

$$as - 1 = m(-t),$$

that is, $m \mid as - 1$ and so $as \equiv 1 \pmod{m}$. Let $a^* = s \bmod m$. Then $a^* \equiv s \pmod{m}$ so $aa^* \equiv 1 \pmod{m}$ and clearly $0 < a^* < m$.

To show uniqueness assume that $ac \equiv 1 \pmod{m}$ and $0 < c < m$. Then $ac \equiv aa^* \pmod{m}$. So if we multiply both sides of this congruence on the left by c and use the fact that $ca \equiv 1 \pmod{m}$ we obtain $c \equiv a^* \pmod{m}$. It follows from Exercise 15.5 that $c = a^*$. □

Remark 18.1. From the above proof we see that Blankinship's Method may be used to compute the inverse of a when it exists, but for small m we may often find a^* by "trial and error." For example, if $m = 15$ take $a = 2$. Then we can check each element $0, 1, 2, \ldots, 14$:

$$\begin{aligned}
2 \cdot 0 &\not\equiv 1 \pmod{15} \\
2 \cdot 1 &\not\equiv 1 \pmod{15} \\
2 \cdot 2 &\not\equiv 1 \pmod{15} \\
2 \cdot 3 &\not\equiv 1 \pmod{15} \\
2 \cdot 4 &\not\equiv 1 \pmod{15} \\
2 \cdot 5 &\not\equiv 1 \pmod{15} \\
2 \cdot 6 &\not\equiv 1 \pmod{15} \\
2 \cdot 7 &\not\equiv 1 \pmod{15} \\
2 \cdot 8 &\equiv 1 \pmod{15} \text{ since } 15 \mid 16 - 1.
\end{aligned}$$

So we can take $2^* = 8$.

Exercise 18.1. Show that the inverse of 2 modulo 7 is not the inverse of 2 modulo 15.

Theorem 18.2. *Let $m > 0$. If $ab \equiv 1 \pmod{m}$ then both a and b are relatively prime to m.*

Proof. If $ab \equiv 1 \pmod{m}$, then $m \mid ab - 1$. So $ab - 1 = mt$ for some t. Hence,

$$ab + m(-t) = 1.$$

By Exercise 9.2 on page 30, this implies that $\gcd(a, m) = 1$ and $\gcd(b, m) = 1$, as claimed. $\square$

Corollary 18.1. *a has an inverse modulo m if and only if a and m are relatively prime.*

Theorem 18.3 (Cancellation). *Let $m > 0$ and assume that $\gcd(c, m) = 1$. Then*

$$(*) \qquad ca \equiv cb \pmod{m} \Rightarrow a \equiv b \pmod{m}.$$

Proof. If $\gcd(c, m) = 1$, there is an integer c^* such that $c^*c \equiv 1 \pmod{m}$. Now since $c^* \equiv c^* \pmod{m}$ and $ca \equiv cb \pmod{m}$ by Theorem 15.3, p. 61,

$$c^*ca \equiv c^*cb \pmod{m}.$$

But $c^*c \equiv 1 \pmod{m}$ so

$$c^*ca \equiv a \pmod{m}$$

and

$$c^*cb \equiv b \pmod{m}.$$

By reflexivity and transitivity this yields

$$a \equiv b \pmod{m}.$$

□

Exercise 18.2. Find specific positive integers a, b, c and m such that $c \not\equiv 0 \pmod{m}$, $\gcd(c, m) > 0$, and $ca \equiv cb \pmod{m}$, but $a \not\equiv b \pmod{m}$.

Although $(*)$ above is not generally true when $\gcd(c, m) > 1$, we do have the following more general kinds of "cancellation:"

Theorem 18.4. *If $c > 0$, $m > 0$ then*

$$a \equiv b \pmod{m} \Leftrightarrow ca \equiv cb \pmod{cm}.$$

Exercise 18.3. Prove Theorem 18.4.

Theorem 18.5. *Let $m > 0$ and let $d = \gcd(c, m)$. Then*

$$ca \equiv cb \pmod{m} \Rightarrow a \equiv b \pmod{\frac{m}{d}}.$$

Proof. Since $d = \gcd(c, m)$ we can write $c = d(\frac{c}{d})$ and $m = d(\frac{m}{d})$. Then $\gcd(\frac{c}{d}, \frac{m}{d}) = 1$. Now rewriting $ca \equiv cb \pmod{m}$ we have

$$d\,\frac{c}{d}\,a \equiv d\,\frac{c}{d}\,b \pmod{d\,\frac{m}{d}}.$$

Since $m > 0$, $d > 0$, so by Theorem 18.4 we have

$$\frac{c}{d}\,a \equiv \frac{c}{d}\,b \pmod{\frac{m}{d}}.$$

Now since $\gcd(\frac{c}{d}, \frac{m}{d}) = 1$, by Theorem 18.3

$$a \equiv b \pmod{\frac{m}{d}}.$$

□

Theorem 18.6. *If $m > 0$ and $a \equiv b \pmod{m}$ we have*

$$\gcd(a, m) = \gcd(b, m).$$

Proof. Since $a \equiv b \pmod{m}$ we have $a - b = mt$ for some t. So we can write

$$a = mt + b \tag{1}$$

and

$$b = m(-t) + a. \tag{2}$$

Let $d = \gcd(m, a)$ and $e = \gcd(m, b)$. Since $e \mid m$ and $e \mid b$, from (1) $e \mid a$ so e is a common divisor of m and a. Hence $e \leq d$. Using (2) we see similarly that $d \leq e$. So $d = e$. □

Corollary 18.2. *Let $m > 0$. Let $a \equiv b \pmod{m}$. Then a has an inverse modulo m if and only if b does.*

Proof. Immediate from Theorems 18.1, 18.2 and 18.6. □

Exercise 18.4. Determine whether or not each of the following is true. **Give reasons in each case.**

(1) $x \equiv 3 \pmod{7} \Rightarrow \gcd(x, 7) = 1$

(2) $\gcd(68019, 3) = 3$

(3) $12x \equiv 15 \pmod{35} \Rightarrow 4x \equiv 5 \pmod{7}$

(4) $x \equiv 6 \pmod{12} \Rightarrow \gcd(x, 12) = 6$

(5) $3x \equiv 3y \pmod{17} \Rightarrow x \equiv y \pmod{17}$

(6) $5x \equiv y \pmod{6} \Rightarrow 15x \equiv 3y \pmod{18}$

(7) $12x \equiv 12y \pmod{15} \Rightarrow x \equiv y \pmod{5}$

(8) $x \equiv 73 \pmod{75} \Rightarrow x \bmod 75 = 73$

(9) $x \equiv 73 \pmod{75}$ and $0 \leq x < 75 \Rightarrow x = 73$

(10) There is no integer x such that

$$12x \equiv 7 \pmod{33}.$$

Chapter 19

Residue Classes

Definition 19.1. Let $m > 0$ be given. For each integer a we define

$$[a] = \{x : x \equiv a \pmod{m}\}. \tag{1}$$

In other words, $[a]$ is the set of all integers that are congruent to a modulo m. We call $[a]$ the **residue class of** a **modulo** m. Some people call $[a]$ the *congruence class* or *equivalence class of a modulo m.*

Theorem 19.1. *For $m > 0$ we have*

$$[a] = \{mq + a \mid q \in \mathbb{Z}\}. \tag{2}$$

Proof. $x \in [a] \Leftrightarrow x \equiv a \pmod{m} \Leftrightarrow m \mid x - a \Leftrightarrow x - a = mq$ for some $q \in \mathbb{Z} \Leftrightarrow x = mq + a$ for some $q \in \mathbb{Z}$. So (2) follows from the definition (1). $\square$

Note that $[a]$ really depends on m and it would be more accurate to write $[a]_m$ instead of $[a]$, but this would be too cumbersome. Nevertheless it should be kept clearly in mind that $[a]$ depends on some understood value of m.

Remark 19.1. Two alternative ways to write (2) are

$$[a] = \{mq + a \mid q = 0, \pm 1, \pm 2, \dots\} \tag{3}$$

or

$$[a] = \{\dots, -2m + a, -m + a, a, m + a, 2m + a, \dots\}. \tag{4}$$

Exercise 19.1. Show that if $m = 2$ then [1] is the set of all odd integers and [0] is the set of all even integers. Show also that $\mathbb{Z} = [0] \cup [1]$ and $[0] \cap [1] = \emptyset$.

Exercise 19.2. Show that if $m = 3$, then [0] is the set of integers divisible by 3, [1] is the set of integers whose remainder when divided by 3 is 1, and [2] is the set of integers whose remainder when divided by 3 is 2. Show also that $\mathbb{Z} = [0] \cup [1] \cup [2]$ and $[0] \cap [1] = [0] \cap [2] = [1] \cap [2] = \emptyset$.

Theorem 19.2. *For a given modulus $m > 0$ we have:*

$$[a] = [b] \Leftrightarrow a \equiv b \pmod{m}.$$

Proof. "$\Rightarrow$" Assume $[a] = [b]$. Note that since $a \equiv a \pmod{m}$ we have $a \in [a]$. Since $[a] = [b]$ we have $a \in [b]$. By definition of $[b]$ this gives $a \equiv b \pmod{m}$, as desired.

"$\Leftarrow$" Assume $a \equiv b \pmod{m}$. We must prove that the sets $[a]$ and $[b]$ are equal. To do this we prove that every element of $[a]$ is in $[b]$ and vice-versa. Let $x \in [a]$. Then $x \equiv a \pmod{m}$. Since $a \equiv b \pmod{m}$, by transitivity $x \equiv b \pmod{m}$ so $x \in [b]$. Conversely, if $x \in [b]$, then $x \equiv b \pmod{m}$. By symmetry since $a \equiv b \pmod{m}$, $b \equiv a \pmod{m}$, so again by transitivity $x \equiv a \pmod{m}$ and $x \in [a]$. This proves that $[a] = [b]$. $\square$

Theorem 19.3. *Given $m > 0$. For every a there is a unique r such that*

$$[a] = [r] \quad \text{and } 0 \leq r < m.$$

Proof. Let $r = a \bmod m$. Then by Exercise 15.1 (p. 59) we have $a \equiv r \pmod{m}$. By definiton of $a \bmod m$ we have $0 \leq r < m$. Since $a \equiv r \pmod{m}$ by Theorem 19.2, $[a] = [r]$. To prove that r is unique, suppose also $[a] = [r']$ where $0 \leq r' < m$. By Theorem 19.2 this implies that $a \equiv r' \pmod{m}$. This, together with $0 \leq r' < m$, implies by Theorem 15.4 that $r' = a \bmod m = r$. $\square$

Theorem 19.4. *Given $m > 0$, there are exactly m distinct residue classes modulo m, namely,*

$$[0], [1], [2], \ldots, [m-1].$$

Proof. By Theorem 19.3 we know that every residue class $[a]$ is equal to one of the residue classes: $[0], [1], \ldots, [m-1]$. So there are no residue classes not in this list. These residue classes are distinct by the uniqueness part of Theorem 19.3, namely if $0 \leq r_1 < m$ and $0 \leq r_2 < m$ and $[r_1] = [r_2]$, then by the uniqueness part of Theorem 19.3 we must have $r_1 = r_2$. $\square$

Exercise 19.3. Given the modulus $m > 0$ show that $[a] = [a+m]$ and $[a] = [a-m]$ for all a.

Exercise 19.4. For any $m > 0$, show that if $x \in [a]$ then $[a] = [x]$.

Definition 19.2. Any element $x \in [a]$ is said to be a *representative* of the residue class $[a]$.

By Exercise 19.4 if x is a representative of $[a]$ then $[x] = [a]$, that is, *any element of a residue class may be used to represent it.*

Exercise 19.5. For any $m > 0$, show that if $[a] \cap [b] \neq \emptyset$ then $[a] = [b]$.

Exercise 19.6. For any $m > 0$, show that if $[a] \neq [b]$ then $[a] \cap [b] = \emptyset$.

Exercise 19.7. Let $m = 2$. Show that

$$[0] = [2] = [4] = [32] = [-2] = [-32]$$

and

$$[1] = [3] = [-3] = [31] = [-31].$$

Chapter 20

$\mathbb{Z}_m$ and Complete Residue Systems

Throughout this section we assume a fixed modulus $m > 0$.

Definition 20.1. We define

$$\mathbb{Z}_m = \{[a] \mid a \in \mathbb{Z}\},$$

that is, $\mathbb{Z}_m$ is the set of all residue classes modulo m. We call $\mathbb{Z}_m$ *the ring of integers modulo m*. In the next chapter we shall show how to add and multiply residue classes. This makes $\mathbb{Z}_m$ into a *ring*. See Appendix A for the definition of *ring*. Often we drop the *ring* and just call $\mathbb{Z}_m$ *the integers modulo m*. From Theorem 19.4

$$\mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}$$

and since no two of the residue classes $[0], [1], \ldots, [m-1]$ are equal we see that $\mathbb{Z}_m$ has exactly m elements. By Exercise 19.4 if we choose

$$a_0 \in [0], a_1 \in [1], \ldots, a_{m-1} \in [m-1]$$

then

$$[a_0] = [0], [a_1] = [1], \ldots, [a_{m-1}] = [m-1].$$

So we also have

$$\mathbb{Z}_m = \{[a_0], [a_1], \ldots, [a_{m-1}]\}.$$

Example 20.1. If $m = 4$ we have, for example,

$$8 \in [0], 5 \in [1], -6 \in [2], 11 \in [3].$$

And hence:

$$\mathbb{Z}_4 = \{[8], [5], [-6], [11]\}.$$

Definition 20.2. A set of m integers

$$\{a_0, a_1, \ldots, a_{m-1}\}$$

is called a *complete residue system modulo m* if

$$\mathbb{Z}_m = \{[a_0], [a_1], \ldots, [a_{m-1}]\}.$$

Remark 20.1. A complete residue system modulo m is sometimes called a *complete set of representatives for $\mathbb{Z}_m$*.

Example 20.2. By Theorem 19.4, p. 76, for $m > 0$

$$\{0, 1, 2, \ldots, m - 1\}$$

is a complete residue system modulo m.

Example 20.3. From the above discussion it is clear that for each $m > 0$ there are infinitely many distinct complete residue systems modulo m. For example, here are some examples of complete residue systems modulo 5:

1. $\{0, 1, 2, 3, 4\}$
2. $\{0, 1, 2, -2, -1\}$
3. $\{10, -9, 12, 8, 14\}$
4. $\{0 + 5n_1, 1 + 5n_2, 2 + 5n_3, 3 + 5n_4, 4 + 5n_4\}$ where n_1, n_2, n_3, n_4, n_5 may be *any* integers.

Definition 20.3. The set $\{0, 1, \ldots, m - 1\}$ is called the set of *least nonnegative residues modulo m*.

Theorem 20.1. *Let $m > 0$ be given.*

(1) *If* $m = 2k$, *then*

$$\{0, 1, 2, \ldots, k-1, k, -(k-1), \ldots, -2, -1\}$$

is a complete residue system modulo m.

(2) *If* $m = 2k+1$, *then*

$$\{0, 1, 2, \ldots, k, -k, \ldots, -2, -1\}$$

is a complete residue system modulo m.

Proof of (1). Since if $m = 2k$

$$\mathbb{Z}_m = \{[0], [1], \ldots, [k], [k+1], \ldots, [k+i], [k+k-1]\},$$

it suffices to note that by Exercise 19.3 we have

$$[k+i] = [k+i-2k] = [-k+i] = [-(k-i)].$$

So

$$[k+1] = [-(k-1)], [k+2] = [-(k-2)], \ldots, [k+k-1] = [-1],$$

as desired. □

Proof of (2). In this case

$$[k+i] = [-(2k+1)+k+i] = [-k+i+1] = [-(k-i+1)]$$

so

$$[k+1] = [-k], [k+2] = [-(k-1)], \ldots, [2k] = [-1],$$

as desired. □

Definition 20.4. The complete residue system modulo m given in Theorem 20.1 is called the *least absolute residue system modulo* m.

Remark 20.2. If one chooses in each residue class $[a]$ the smallest nonnegative integer one obtains the *least nonnegative residue system*. If one chooses in each residue class $[a]$ an element of smallest possible absolute value one obtains the *least absolute residue system*.

Exercise 20.1. Find both the least nonnegative residue system and the least absolute residues for each of the moduli given below. Also, in each case find a *third* complete residue system *different* from these two.

$$m = 3, \quad m = 4, \quad m = 5, \quad m = 6, \quad m = 7, \quad m = 8.$$

Chapter 21

Addition and Multiplication in $\mathbb{Z}_m$

In this chapter we show how to define addition and multiplication of residue classes modulo m. With respect to these binary operations $\mathbb{Z}_m$ is a *ring* as defined in Appendix A.

Definition 21.1. For $[a], [b] \in \mathbb{Z}_m$ we define

$$[a] + [b] = [a + b]$$

and

$$[a][b] = [ab].$$

Example 21.1. For $m = 5$ we have

$$[2] + [3] = [5],$$

and

$$[2][3] = [6].$$

Note that since $5 \equiv 0 \pmod 5$ and $6 \equiv 1 \pmod 5$ we have $[5] = [0]$ and $[6] = [1]$ so we can also write

$$[2] + [3] = [0]$$
$$[2][3] = [1].$$

Since a residue class can have many representatives, it is important to check that the rules given in Definition 21.1 do not depend on the representatives chosen. For example, when $m = 5$ we know that

$$[7] = [2] \text{ and } [11] = [21]$$

so we *should* have

$$[7] + [11] = [2] + [21]$$

and

$$[7][11] = [2][21].$$

In this case we can check that

$$[7] + [11] = [18] \text{ and } [2] + [21] = [23].$$

Now $23 \equiv 18 \pmod 5$ since $5 \mid 23 - 18$. Hence $[18] = [23]$, as desired. Also $[7][11] = [77]$ and $[2][21] = [42]$. Then $77 - 42 = 35$ and $5 \mid 35$ so $77 \equiv 42 \pmod 5$ and hence $[77] = [42]$, as desired.

Theorem 21.1. *For any modulus $m > 0$ if $[a] = [b]$ and $[c] = [d]$ then*

$$[a] + [c] = [b] + [d]$$

and

$$[a][c] = [b][d].$$

Proof. (This follows immediately from Theorem 15.3 (p. 61) and Theorem 19.2 (p. 76).) □

Exercise 21.1. Prove Theorem 21.1.

When performing addition and multiplication in $\mathbb{Z}_m$ using the rules in Definition 21.1, due to Theorem 21.1, we may at any time replace $[a]$ by $[a']$ if $a \equiv a' \pmod m$. This will sometimes make calculations easier.

Example 21.2. Take $m = 151$. Then $150 \equiv -1 \pmod{151}$ and $149 \equiv -2 \pmod{151}$, so

$$[150][149] = [-1][-2] = [2]$$

and

$$[150] + [149] = [-1] + [-2] = [-3] = [148]$$

since $148 \equiv -3 \pmod{151}$.

When working with $\mathbb{Z}_m$ it is often useful to write all residue classes in the least nonnegative residue system, as we do in constructing the following addition and multiplication tables for $\mathbb{Z}_4$.

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

Recall that by Exercise 15.1 (p. 59) we have for all a and $m > 0$

$$a \equiv a \bmod m \pmod{m}.$$

So using residue classes modulo m this gives

$$[a] = [a \bmod m].$$

Hence,

$$\boxed{\begin{aligned}[][a] + [b] &= [(a+b) \bmod m]\\ [a][b] &= [(ab) \bmod m]\end{aligned}}$$

So if a and b are in the set $\{0, 1, \ldots, m-1\}$, these equations give us a way to obtain representations of the sum and product of $[a]$ and $[b]$ in the same set. This leads to an alternative way to define $\mathbb{Z}_m$ and addition and multiplication in $\mathbb{Z}_m$. For clarity we will use different notation.

Definition 21.2. For $m > 0$ define

$$J_m = \{0, 1, 2, \ldots, m-1\}$$

and for $a, b \in J_m$ define

$$\begin{aligned} a \oplus b &= (a+b) \bmod m \\ a \odot b &= (ab) \bmod m. \end{aligned}$$

Remark 21.1. J_m with $\oplus$ and $\odot$ as defined is **isomorphic** to $\mathbb{Z}_m$ with addition and multiplication given by Definition 21.1. [Students taking Elementary Abstract Algebra will learn a rigorous definition of the term isomorphic. For now, we take "isomorphic" to mean "has the same form."] The addition and multiplication tables for J_4 are:

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\odot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Exercise 21.2. Prove that for every modulus $m > 0$ we have for all $a, b \in J_m$

$$[a] + [b] = [a \oplus b],$$

and

$$[a][b] = [a \odot b].$$

Exercise 21.3. Construct addition and multiplication tables for J_5.

Exercise 21.4. *Without doing it*, tell how to obtain addition and multiplication tables for $\mathbb{Z}_5$ from the work in Exercise 21.3.

Example 21.3. Let's solve the congruence

$$272x \equiv 901 \pmod{9}. \tag{1}$$

Using residue classes modulo 9 we see that (1) is equivalent to

$$[272x] = [901] \tag{2}$$

which is equivalent to

$$[272][x] = [901] \tag{3}$$

which is equivalent to

$$[2][x] = [1]. \tag{4}$$

Now we know $[x] \in \{[0], [1], \ldots, [8]\}$ so by trial and error we see that $x = 5$ is a solution.

Chapter 22

The Groups U_m

Definition 22.1. Let $m > 0$. A residue class $[a] \in \mathbb{Z}_m$ is called a **unit** if there is another residue class $[b] \in \mathbb{Z}_m$ such that $[a][b] = [1]$. In this case $[a]$ and $[b]$ are said to be *inverses of each other* in $\mathbb{Z}_m$.

Theorem 22.1. *Let $m > 0$. A residue class $[a] \in \mathbb{Z}_m$ is a unit if and only if* $\gcd(a, m) = 1$.

Proof. Let $[a]$ be a unit. Then there is some $[b]$ such that $[a][b] = [1]$. Hence $[ab] = [1]$ so $ab \equiv 1 \pmod{m}$. So by Theorem 18.2, p. 72, $\gcd(a, m) = 1$.

To prove the converse, let $\gcd(a, m) = 1$. Then by Theorem 18.1, page 71, there is an integer a^* such that $aa^* \equiv 1 \pmod{m}$. Hence, $[aa^*] = [1]$. So $[a][a^*] = [aa^*] = [1]$, and we can take $b = a^*$. □

Note that from Theorem 18.6 we see that if $[a] = [b]$ (i.e., $a \equiv b \pmod{m}$) then $\gcd(a, m) = 1 \Leftrightarrow \gcd(b, m) = 1$. So in checking whether or not a residue class is a unit we can use any representative of the class.

Exercise 22.1. Show that $[1]$ and $[m-1]$ are always units in $\mathbb{Z}_m$. Hint: $[m-1] = [-1]$.

Definition 22.2. The set of all units in $\mathbb{Z}_m$ is denoted by U_m and is called the *group of units* of $\mathbb{Z}_m$. See Appendix A for the definition of a *group*.

Theorem 22.2. *Let $m > 0$, then*

$$U_m = \{[i] \mid 1 \le i \le m \text{ and } \gcd(i, m) = 1\}.$$

Proof. We know that if $[a] \in \mathbb{Z}_m$ then $[a] = [i]$ where $0 \leq i \leq m-1$. If $m = 1$ then $\mathbb{Z}_m = \mathbb{Z}_1 = \{[0]\} = \{[1]\}$ and since $[1][1] = [1]$, $[1]$ is a unit, $U_1 = \{[1]\}$ and the theorem holds. If $m \geq 2$, then $\gcd(i, m) = 1$ can only happen if $1 \leq i \leq m-1$, since $\gcd(0, m) = \gcd(m, m) = m \neq 1$. So the theorem follows from Theorem 22.1 and the above remarks. ☐

Theorem 22.3. *(U_m is a group [1] under multiplication.)*

(1) *If* $[a], [b] \in U_m$ *then* $[a][b] \in U_m$.

(2) *For all* $[a]$, $[b]$, $[c]$ *in* U_m *we have* $([a][b])[c] = [a]([b][c])$.

(3) $[1][a] = [a][1] = [a]$ *for all* $[a] \in U_m$.

(4) *For each* $[a] \in U_m$ *there is a* $[b] \in U_m$ *such that* $[a][b] = [1]$.

(5) *For all* $[a], [b] \in U_m$ *we have* $[a][b] = [b][a]$.

Exercise 22.2. Prove Theorem 22.3.

Example 22.1. Using Theorem 22.2 we see that

$$\begin{aligned} U_{15} &= \{[1], [2], [4], [7], [8], [11], [13], [14]\} \\ &= \{[1], [2], [4], [7], [-7], [-4], [-2], [-1]\}. \end{aligned}$$

Note that using absolute least residue modulo 15 simplifies multiplication somewhat. Rather than write out the entire multiplication table, we just find the inverse of each element of U_{15}:

$$\begin{gathered} [1][1] = [1] \\ [2][-7] = [2][8] = [1] \\ [4][4] = [1] \\ [7][-2] = [7][13] = [1] \\ [-4][-4] = [11][11] = [1] \\ [-1][-1] = [14][14] = [1]. \end{gathered}$$

Exercise 22.3. Find the elements of U_7 in *both* least nonnegative and absolute least residue form and find the inverse of each element, as in the example above.

[1] Actually (1)–(4) are all that is required for U_n to be a **group**. Property (5) says that U_n is an **Abelian** group. See Appendix A.

Definition 22.3. If X is a set, the number of elements in X is denoted by $|X|$.

Example 22.2. $|\{1\}| = 1$, $|\{0,1,3,9\}| = 4$, $|\mathbb{Z}_m| = m$ if $m > 0$.

Definition 22.4. If $m \geq 1$,

$$\phi(m) = |\{i \in \mathbb{Z} \mid 1 \leq i \leq m \text{ and } \gcd(i,m) = 1\}|.$$

The function ϕ is called the *Euler phi function* or the *Euler totient function.*

Corollary 22.1. *If $m > 0$,*

$$|U_m| = \phi(m).$$

Note that

$$\begin{aligned}
U_1 &= \{[1]\} \text{ so } \phi(1) = 1 \\
U_2 &= \{[1]\} \text{ so } \phi(2) = 1 \\
U_3 &= \{[1],[2]\} \text{ so } \phi(3) = 2 \\
U_4 &= \{[1],[3]\} \text{ so } \phi(4) = 2 \\
U_5 &= \{[1],[2],[3],[4]\} \text{ so } \phi(5) = 4 \\
U_6 &= \{[1],[5]\} \text{ so } \phi(6) = 2 \\
U_7 &= \{[1],[2],[3],[4],[5],[6]\} \text{ so } \phi(7) = 6.
\end{aligned}$$

Generally $\phi(m)$ is not easy to calculate. However, the following theorems show that once the prime factorization of m is given, computing $\phi(m)$ is easy.

Theorem 22.4. *If $a > 0$ and $b > 0$ and $\gcd(a,b) = 1$, then*

$$\phi(ab) = \phi(a)\phi(b).$$

Theorem 22.5. *If p is prime and $n > 0$ then*

$$\phi(p^n) = p^n - p^{n-1}.$$

Theorem 22.6. *Let $p_1, p_2, \ldots, p_k$ be distinct primes and let $n_1, n_2, \ldots, n_k$ be positive integers, then*

$$\phi\left(p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}\right) = \left(p_1^{n_1} - p_1^{n_1-1}\right) \cdots \left(p_k^{n_k} - p_k^{n_k-1}\right).$$

Before discussing the proofs of these three theorems, let's illustrate their use:

$$\begin{aligned}\phi(12) &= \phi\left(2^2 \cdot 3\right) = \left(2^2 - 2^1\right)\left(3^1 - 3^0\right) = 2 \cdot 2 = 4 \\ \phi(9000) &= \phi\left(2^3 \cdot 5^3 \cdot 3^2\right) = \left(2^3 - 2^2\right)\left(5^3 - 5^2\right)\left(3^2 - 3^1\right) \\ &= 4 \cdot 100 \cdot 6 = 2400.\end{aligned}$$

Note that if p is any prime then

$$\phi(p) = p - 1.$$

I will sketch a proof of Theorem 22.4 in Exercise 22.6 below. Now I give the proof of Theorem 22.5.

Proof of Theorem 22.5. We want to count the number of elements in the set $A = \{1, 2, \ldots, p^n\}$ that are relatively prime to p^n. Let B be the set of elements of A that have a factor > 1 in common with A. Note that if $b \in B$ and $\gcd(b, p^n) = d > 1$, then d is a factor of p^n and $d > 1$ so d has p as a factor. Hence $b = pk$, for some k, and $p \leq b \leq p^n$, so $p \leq kp \leq p^n$. It follows that $1 \leq k \leq p^{n-1}$. That is,

$$B = \left\{p, 2p, 3p, \ldots, kp, \ldots, p^{n-1}p\right\}.$$

We are interested in the number of elements of A not in B. Since $|A| = p^n$ and $|B| = p^{n-1}$, this number is $p^n - p^{n-1}$. That is, $\phi(p^n) = p^n - p^{n-1}$. □

The proof of Theorem 22.6 follows from Theorems 22.4 and 22.5. The proof is by induction on n and is quite similar to the proof of Theorem 13.1 (2) on page 50, so I omit the details.

Exercise 22.4. Find the sets U_m, for $8 \leq m \leq 20$. Note that $|U_m| = \phi(m)$. Use Theorem 22.6 to calculate $\phi(m)$ and check that you have the right number of elements for each set U_m, $8 \leq m \leq 20$.

Exercise 22.5. Show that if

$$m = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$$

where $p_1, \ldots, p_k$ are distinct primes and each $n_i \geq 1$, then

$$\phi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Exercise 22.6. Let a and b be relatively prime positive integers. Write $n = ab$. Define the mapping f by the rule

$$f([x]_n) = ([x]_a, [x]_b).$$

Here we denote the residue class of x modulo m by $[x]_m$. First illustrate each of the following for the special case $a = 3$ and $b = 5$. Then prove each in general. (The proof is difficult and is optional.)

1. $f : \mathbb{Z}_n \to \mathbb{Z}_a \times \mathbb{Z}_b$ is one-to-one and onto. (This is called the *Chinese Remainder Theorem.*)

2. $f : U_n \to U_a \times U_b$ is also a one-to-one, onto mapping.

3. Conclude from (2) that $\phi(ab) = \phi(a)\phi(b)$.

Chapter 23

Two Theorems of Euler and Fermat

Fermat's Big Theorem or, as it is also called, *Fermat's Last Theorem* states that $x^n + y^n = z^n$ has no solutions in positive integers x, y, z when $n > 2$. This was proved by Andrew Wiles in 1995 over 350 years after it was first mentioned by Fermat. The theorem that concerns us in this chapter is *Fermat's Little Theorem.* This theorem is much easier to prove, but has more far reaching consequences for applications to cryptography and secure transmission of data on the Internet. The first theorem below is a generalization of Fermat's Little Theorem due to Euler.

Theorem 23.1 (Euler's Theorem). *If $m > 0$ and a is relatively prime to m then*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Theorem 23.2 (Fermat's Little Theorem). *If p is prime and a is relatively prime to p then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Let's look at some examples. Take $m = 12$ then

$$\phi(m) = \phi\left(2^2 \cdot 3\right) = \left(2^2 - 2\right)(3 - 1) = 4.$$

The positive integers $a < m$ with $\gcd(a, m) = 1$ are 1, 5, 7 and 11.

$$\begin{aligned} 1^4 &\equiv 1 \pmod{12} \quad \text{is clear} \\ 5^2 &\equiv 1 \pmod{12} \quad \text{since } 12 \mid 25 - 1 \\ \therefore \left(5^2\right)^2 &\equiv 1^2 \pmod{12} \\ \therefore 5^4 &\equiv 1 \pmod{12}. \end{aligned}$$

Now $7 \equiv -5 \pmod{12}$ and since 4 is even

$$\begin{aligned} 7^4 &\equiv 5^4 \pmod{12} \\ \therefore 7^4 &\equiv 1 \pmod{12}. \end{aligned}$$

$11 \equiv -1 \pmod{12}$ and again since 4 is even we have

$$11^4 \equiv (-1)^4 \pmod{12}$$

and

$$11^4 \equiv 1 \pmod{12}.$$

So we have verified Theorem 23.1 for the single case $m = 12$.

Exercise 23.1. Verify that Theorem 23.2 holds if $p = 5$ by direct calculation as in the above example.

Definition 23.1. (Powers of residue classes.) If $[a] \in U_m$ define $[a]^1 = [a]$ and for $n > 1$, $[a]^n = [a][a] \cdots [a]$ where there are n copies of $[a]$ on the right.

Theorem 23.3. *If $[a] \in U_m$, then $[a]^n \in U_m$ for $n \geq 1$ and $[a]^n = [a^n]$.*

Proof. We prove that $[a]^n = [a^n] \in U_m$ for $n \geq 1$ by induction on n.

If $n = 1$, $[a]^1 = [a] = [a^1]$ and by assumption $[a] \in U_m$. Suppose

$$[a]^k = \left[a^k\right] \in U_m$$

for some $k \geq 1$. Then

$$\begin{aligned} [a]^{k+1} &= [a]^k [a] \\ &= \left[a^k\right][a] \quad \text{by the induction hypothesis} \\ &= \left[a^k a\right] \quad \text{by Definition 21.1, p. 83} \\ &= \left[a^{k+1}\right] \quad \text{since } a^k a = a^{k+1}. \end{aligned}$$

So by the PMI, the theorem holds for $n \geq 1$. $\square$

Note that for fixed $m > 0$ if $\gcd(a, m) = 1$ then $[a] \in U_m$. And using Theorem 23.3 we have

$$a^n \equiv 1 \pmod{m} \iff [a^n] = [1] \iff [a]^n = [1].$$

It follows that Euler's Theorem (Theorem 23.1) is equivalent to the following theorem.

Theorem 23.4. *If $m > 0$ and $[a] \in U_m$ then*

$$[a]^{\phi(m)} = [1].$$

A proof of Theorem 23.4 is outlined in the following exercise.

Exercise 23.2 (Optional). Let $U_m = \{X_1, X_2, \dots, X_{\phi(m)}\}$. Here we write X_i for a residue class in U_m to simplify notation.

1. Show that if $X \in U_m$ then

$$\{XX_1, XX_2, \cdots, XX_{\phi(m)}\} = U_m.$$

2. Show that if $X \in U_m$ then

$$XX_1XX_2 \cdots XX_{\phi(m)} = X_1X_2 \cdots X_{\phi(m)}.$$

3. Let $A = X_1X_2 \cdots X_{\phi(m)}$. Show that if $X \in U_m$ then $X^{\phi(m)}A = A$.

4. Conclude from (3) that $X^{\phi(m)} = [1]$ and hence Theorem 23.4 is true.

Also Theorem 23.4 is an easy consequence of *Lagrange's Theorem*, which students who take (or have taken) a course in abstract algebra will learn about (or will already know).

Exercise 23.3. Show that Fermat's Little Theorem follows from Euler's Theorem.

Exercise 23.4. Show that if p is prime then $a^p \equiv a \pmod{p}$ for all integers a. Hint: Consider two cases: I. $\gcd(a, p) = 1$ and II. $\gcd(a, p) > 1$. Note that in the second case $p \mid a$.

Exercise 23.5. Let $m > 0$. Let $\gcd(a, m) = 1$. Show that $a^{\phi(m)-1}$ is an inverse for a modulo m. (See Theorem 18.1, p. 71.)

Exercise 23.6. For all $a \in \{1, 2, 3, 4, 5, 6\}$ find the inverse a^* of a modulo 7 by use of Exercise 23.5. Choose a^* in each case so that $1 \leq a^* \leq 6$.

Example 23.1. Note that Fermat's Little Theorem can be used to simplify the computation of $a^n \bmod p$ where p is prime. Recall that if $a^n \equiv r \pmod{p}$ where $0 \leq r < p$, then $a^n \bmod p = r$. We can do two things to simplify the computation:

(1) Replace a by $a \bmod p$.

(2) Replace n by $n \bmod (p-1)$.

Suppose we want to calculate

$$1234^{7865435} \bmod 11.$$

Note that $1234 \equiv -1+2-3+4 \pmod{11}$, that is, $1234 \equiv 2 \pmod{11}$. Since $\gcd(2, 11) = 1$ we have $2^{10} \equiv 1 \pmod{11}$. Now $7865435 = (786543) \cdot 10 + 5$ so

$$\begin{aligned} 2^{7865435} &\equiv 2^{(786543)\cdot 10+5} \pmod{11} \\ &\equiv \left(2^{10}\right)^{786543} \cdot 2^5 \pmod{11} \\ &\equiv 1^{786543} \cdot 2^5 \pmod{11} \\ &\equiv 2^5 \pmod{11}, \end{aligned}$$

and $2^5 = 32 \equiv 10 \pmod{11}$. Hence,

$$1234^{7865435} \equiv 10 \pmod{11}.$$

It follows that

$$1234^{7865435} \bmod 11 = 10.$$

Exercise 23.7. Use the technique in the above example to calculate

$$28^{1202} \bmod 13.$$

[Here you cannot use the mod 11 trick, of course.]

Chapter 24

Probabilistic Primality Tests

According to Fermat's Little Theorem, if p is prime and $1 \leq a \leq p-1$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

The converse is also true in the following sense:

Theorem 24.1. *If $m \geq 2$ and for all a such that $1 \leq a \leq m-1$ we have*

$$a^{m-1} \equiv 1 \pmod{m}$$

then m must be prime.

Proof. If the hypothesis holds, then for all a with $1 \leq a \leq m-1$, we know that a has an inverse modulo m, namely, a^{m-2} is an inverse for a modulo m. By Theorem 18.2, this says that for $1 \leq a \leq m-1$, $\gcd(a, m) = 1$. But if m were not prime, then we would have $m = ab$ with $1 < a < m$, $1 < b < m$. Then $\gcd(a, m) = a > 1$, a contradiction. So m must be prime. □

Using the above theorem to check that p is prime we would have to check that $a^{p-1} \equiv 1 \pmod{p}$ for $a = 1, 2, 3, \ldots, p-1$. This is a lot of work. Suppose we just know that $2^{m-1} \equiv 1 \pmod{m}$ for some $m > 2$. Must m be prime? Unfortunately, the answer is no.The smallest composite m satisfying $2^{m-1} \equiv 1 \pmod{m}$ is $m = 341$.

Exercise 24.1. Use Maple (or do it via hand and or calculator) to verify that $2^{340} \equiv 1 \pmod{341}$ and that 341 is not prime.

The moral is that even if $2^{m-1} \equiv 1 \pmod{m}$, the number m need not be prime.

On the other hand, consider the case of $m = 63$. Note that

$$2^6 = 64 \equiv 1 \pmod{63}.$$

Hence, $2^6 \equiv 1 \pmod{63}$. Raising both sides to the 10th power we have

$$2^{60} \equiv 1 \pmod{63}.$$

Then multiplying both sides by 2^2 we get

$$2^{62} \equiv 4 \pmod{63}$$

since

$$4 \not\equiv 1 \pmod{63}$$

we have

$$\boxed{2^{62} \not\equiv 1 \pmod{63}.}$$

This tells us that 63 is *not* prime, *without factoring* 63. We emphasize that in general if $2^{m-1} \not\equiv 1 \pmod{m}$ then we can be sure that m is not prime.

FACT. There are 455,052,511 odd primes $p \leq 10^{10}$, all of which satisfy $2^{p-1} \equiv 1 \pmod{p}$. There are only 14,884 composite numbers $2 < m \leq 10^{10}$ that satisfy $2^{m-1} \equiv 1 \pmod{m}$. Thus, if $2 < m \leq 10^{10}$ and m satisfies $2^{m-1} \equiv 1 \pmod{m}$, the probability m is prime is

$$\frac{455,052,511}{455,052,511 + 14,884} \approx .999967292.$$

In other words, if you find that $2^{m-1} \equiv 1 \pmod{m}$, then it is highly likely (but not a certainty) that m is prime, at least when $m \leq 10^{10}$. Thus the following Maple procedure will almost always give the correct answer:

```
> is_prob_prime:=proc(n)
    if n <=1  or Power(2,n-1) mod n <> 1 then
       return "not prime";
    else
       return "probably prime";
    end if;
  end proc:
```

Note that the Maple command `Power(a,n-1) mod n` is an efficient way to compute $a^{n-1} \bmod n$. We discuss this in more detail later. The procedure `is_prob_prime(n)` just defined returns "probably prime" if $2^{n-1} \bmod n = 1$ and "not prime" if $n \leq 1$ or if $2^{n-1} \bmod n \neq 1$. If the answer is "not prime", then we know definitely that n is not prime. If the answer is "probably prime", we know that there is a very small probability that n is not prime.

In practice, there are better probabilistic primality tests than that mentioned above. For more details see, for example, "Elementary Number Theory," Fourth Edition, by Kenneth Rosen.

The built-in Maple procedure `isprime` is a very sophisticated probabilistic primality test. The command `isprime(n)` returns false if n is not prime and returns true if n is probably prime. So far no one has found an integer n for which `isprime(n)` gives the wrong answer.

One might ask what happens if we use 3 instead of 2 in the above probabilistic primality test. Or, better yet, what if we evaluate $a^{m-1} \bmod m$ for several different values of a.

Consider the following data:

The number of primes $\leq 10^6$ is 78,498.

The number of composite numbers $m \leq 10^6$ such that $2^{m-1} \equiv 1 \pmod{m}$ is 245.

The number of composite numbers $m \leq 10^6$ such that $2^{m-1} \equiv 1 \pmod{m}$ and $3^{m-1} \equiv 1 \pmod{m}$ is 66.

The number of composite numbers $m \leq 10^6$ such that $a^{m-1} \equiv 1 \pmod{m}$ for $a \in \{2, 3, 5, 7, 11, 13, 17, 19, 31, 37, 41\}$ is 0.

Thus, we have the following result:

If $m \leq 10^6$ and $a^{m-1} \equiv 1 \pmod{m}$ for $a \in \{2, 3, 5, 7, 11, 17, 19, 31, 37, 41\}$, then m is prime.

The above results for $m \leq 10^6$ were found using Maple.

If $m > 10^6$ and $a^{m-1} \equiv 1 \pmod{m}$ for $a \in \{2, 3, 5, 7, 11, 17, 19, 31, 37, 41\}$, it is highly likely, but not certain, that m is prime. Actually the primality test `isprime` that is built into Maple uses a somewhat different idea.

Exercise 24.2. Use Maple to show that

(1) $3^{90} \equiv 1 \pmod{91}$, but 91 is not prime.

(2) $2^{m-1} \equiv 1 \pmod{m}$ and $3^{m-1} \equiv 1 \pmod{m}$ for $m = 1105$, but 1105 is not prime.

[**Hints.** Note that $a^n \equiv 1 \pmod{m} \Leftrightarrow a^n \bmod m = 1$. In Maple, 3^{90} is written `3^90` and $3^{90} \bmod 91$ is written `3^90 mod 91`. A faster way to compute $a^n \bmod m$ in Maple is to use the command `Power(a,n) mod m` . Recall that `ifactor(m)` is the command to factor m.]

Chapter 25

The Base b Representation of n

Definition 25.1. Let $b \geq 2$ and $n > 0$. We write

$$n = [a_k, a_{k-1}, \ldots, a_1, a_0]_b \tag{1}$$

if and only if for some $k \geq 0$

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$$

where $a_i \in \{0, 1, \ldots, b-1\}$ for $i = 0, 1, \ldots, k$. $[a_k, a_{k-1}, \ldots, a_1, a_0]$ is called a *base b representation of n.*

Remark 25.1. *Base b* is called

$$\begin{aligned} \textit{binary} &\quad \text{if } b = 2, \\ \textit{ternary} &\quad \text{if } b = 3, \\ \textit{octal} &\quad \text{if } b = 8, \\ \textit{decimal} &\quad \text{if } b = 10, \\ \textit{hexadecimal} &\quad \text{if } b = 16. \end{aligned}$$

If b is understood, especially if $b = 10$, we write $a_k a_{k-1} \cdots a_1 a_0$ in place of $[a_k, a_{k-1}, \ldots, a_1, a_0]_{10}$. In the case of $b = 16$, which is used frequently in computer science, the "digits" 10, 11, 12, 13, 14 and 15 are replaced by A, B, C, D, E and F, respectively.

For a fixed base $b \geq 2$, the numbers $a_i \in \{0, 1, 2, \ldots, b-1\}$ in equation (1) are called the *digits* of the base b representation of n. In the binary case $a_i \in \{0, 1\}$ and the a_i's are called *bits* (*bi*nary digi*ts*).

Here are a few examples:

(1) $267 = [5, 3, 1]_7$
since $267 = 5 \cdot 7^2 + 3 \cdot 7 + 1$.

(2) $147 = [1, 0, 0, 1, 0, 0, 1, 1]_2$
since $147 = 1 \cdot 2^7 + 0 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2 + 1$.

(3) $4879 = [4, 8, 7, 9]_{10}$
since $4879 = 4 \cdot 10^3 + 8 \cdot 10^2 + 7 \cdot 10 + 9$.

(4) $10705679 = [A, 3, 5, B, 0, F]_{16}$
since $10705679 = 10 \cdot 16^5 + 3 \cdot 16^4 + 5 \cdot 16^3 + 11 \cdot 16^2 + 0 \cdot 16 + 15$.

(5) $107056791 = [107, 56, 791]_{1000}$
since $107056791 = 107 \cdot 1000^2 + 56 \cdot 1000 + 791$.

Theorem 25.1. *If $b \geq 2$, then every $n > 0$ has a unique base b representation of the form $n = [a_k, \ldots, a_1, a_0]_b$ with $a_k > 0$.*

Proof. Apply repeatedly the Division Algorithm as follows:

$$\begin{aligned}
n &= bq_0 + r_0, \quad 0 \leq r_0 < b \\
q_0 &= bq_1 + r_1, \quad 0 \leq r_1 < b \\
q_1 &= bq_2 + r_2, \quad 0 \leq r_2 < b \\
&\vdots \\
q_{k-1} &= bq_k + r_k, \quad 0 \leq r_k < b \\
q_k &= bq_{k+1} + r_{k+1}, \quad 0 \leq r_{k+1} < b.
\end{aligned}$$

It is easy to see that if $q_k > 0$:

$$n > q_0 > q_1 > \cdots > q_k.$$

Since this cannot go on forever we eventually obtain $q_\ell = 0$ for some ℓ. Then we have

$$q_{\ell-1} = b \cdot 0 + r_\ell.$$

I claim that $n = [r_\ell, r_{\ell-1}, \ldots, r_0]$ if ℓ is the smallest integer such that $q_\ell = 0$. To see this, note that

$$n = bq_0 + r_0$$

and

$$q_0 = bq_1 + r_1.$$

Hence

$$\begin{aligned} n &= b\left(bq_1 + r_1\right) + r_0 \\ n &= b^2 q_1 + br_1 + r_0. \end{aligned}$$

Continuing in this way we find that

$$n = b^{\ell+1} q_\ell + b^\ell r_\ell + \cdots + br_1 + r_0.$$

And, since $q_\ell = 0$ we have

$$(*) \qquad n = b^\ell r_\ell + \cdots + br_1 + r_0,$$

which shows that

$$n = \left[r_\ell, \ldots, r_1, r_0\right]_b.$$

To see that this representation is unique, note that from $(*)$ we have

$$n = b\left(b^{\ell-1} r_\ell + \cdots + r_1\right) + r_0, \quad 0 \le r_0 < b.$$

By the Division Algorithm it follows that r_0 is uniquely determined by n, as is the quotient $q = b^{\ell-1} r_\ell + \cdots + r_1$. A similar argument shows that r_1 is uniquely determined. Continuing in this way we see that all the digits $r_\ell, r_{\ell-1}, \ldots, r_0$ are uniquely determined. □

Example 25.1.

(1) We find the base 7 representation of 1,749.

$$\begin{aligned} 1749 &= 249 \cdot 7 + 6 \\ 249 &= 35 \cdot 7 + 4 \\ 35 &= 5 \cdot 7 + 0 \\ 5 &= 0 \cdot 7 + 5 \end{aligned}$$

Hence $1749 = [5, 0, 4, 6]_7$.

(2) We find the base 12 representation of 19,151.

$$\begin{aligned} 19,151 &= 1595 \cdot 12 + 11 \\ 1,595 &= 132 \cdot 12 + 11 \\ 132 &= 11 \cdot 12 + 0 \\ 11 &= 0 \cdot 12 + 11 \end{aligned}$$

$\therefore 19,151 = [11, 0, 11, 11]_{12}$.

(3) Find the base 10 representation of 1,203.

$$\begin{aligned} 1203 &= 120 \cdot 10 + 3 \\ 120 &= 12 \cdot 10 + 0 \\ 12 &= 1 \cdot 10 + 2 \\ 1 &= 0 \cdot 10 + 1 \end{aligned}$$

$\therefore 1203 = [1, 2, 0, 3]_{10}$.

(4) Find the base 2 (*binary*) representation of 137.

$$\begin{aligned} 137 &= 2 \cdot 68 + 1 \\ 68 &= 2 \cdot 34 + 0 \\ 34 &= 2 \cdot 17 + 0 \\ 17 &= 2 \cdot 8 + 1 \\ 8 &= 2 \cdot 4 + 0 \\ 4 &= 2 \cdot 2 + 0 \\ 2 &= 2 \cdot 1 + 0 \\ 1 &= 2 \cdot 0 + 1 \end{aligned}$$

$\therefore 137 = [1, 0, 0, 0, 1, 0, 0, 1]_2$.

Exercise 25.1. Generalize the following observations

$$\begin{aligned} 3 &= [1, 1]_2 \\ 7 &= [1, 1, 1]_2 \\ 15 &= [1, 1, 1, 1]_2 \\ 31 &= [1, 1, 1, 1, 1]_2 \\ 63 &= [1, 1, 1, 1, 1, 1]_2 \end{aligned}$$

Prove your generalization. [HINT: See Exercise 2.5 on page 6.]

Exercise 25.2. Generalize the following observation:

$$\begin{aligned} 8 &= [2,2]_3 \\ 26 &= [2,2,2]_3 \\ 80 &= [2,2,2,2]_3 \\ 242 &= [2,2,2,2,2]_3 \end{aligned}$$

Prove your generalization. [HINT: See Exercise 2.5 on page 6.]

Exercise 25.3. Generalize Exercises 25.1 and 25.2 to an arbitrary base $b \geq 2$.

Remark 25.2. To find the binary representation of a small number, the following method is often easier than the above method:

Given $n > 0$ let 2^{n_1} be the largest power of 2 satisfying $2^{n_1} \leq n$. Let 2^{n_2} be the largest power of 2 satisfying

$$2^{n_2} \leq n - 2^{n_1}.$$

Let 2^{n_3} be the largest power of 2 satisfying

$$2^{n_3} \leq n - 2^{n_1} - 2^{n_2}.$$

Note that at this point we have

$$0 \leq n - (2^{n_1} + 2^{n_2} + 2^{n_3}) < n - (2^{n_1} + 2^{n_2}) < n - 2^{n_1} < n.$$

Continuing in this way, eventually we get

$$0 = n - (2^{n_1} + 2^{n_2} + \cdots + 2^{n_k}).$$

Then $n = 2^{n_1} + 2^{n_2} + \cdots + 2^{n_k}$, and this gives the binary representation of n.

Example 25.2. Take $n = 137$. Note that $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 32$, $2^6 = 64$, $2^7 = 128$, and $2^8 = 256$. Using the above method we compute:

$$\begin{aligned} 137 - 2^7 &= 137 - 128 = 9, \\ 9 - 2^3 &= 1, \\ 1 - 2^0 &= 0. \end{aligned}$$

So we have

$$137 = 2^7 + 9 = 2^7 + 2^3 + 1,$$
$$\therefore 137 = 2^7 + 02^6 + 02^5 + 02^4 + 2^3 + 02^2 + 0 \cdot 2 + 1.$$

So $137 = [1,0,0,0,1,0,0,1]_2$.

Exercise 25.4. Show how to use *both methods* to find the binary representation of 455.

Exercise 25.5. Make a vertical list of the binary representation of the integers 1 to 16.

Chapter 26

Computation of $a^N \bmod m$

Let's first consider the question: *What is the smallest number of multiplications required to compute a^N where N is any positive integer?*

Suppose we want to calculate 2^8. One way is to perform the following 7 multiplications:

$$\begin{aligned}
2^2 &= 2 \cdot 2 = 4 \\
2^3 &= 2 \cdot 4 = 8 \\
2^4 &= 2 \cdot 8 = 16 \\
2^5 &= 2 \cdot 16 = 32 \\
2^6 &= 2 \cdot 32 = 64 \\
2^7 &= 2 \cdot 64 = 128 \\
2^8 &= 2 \cdot 128 = 256
\end{aligned}$$

But we can do it in only 3 multiplications:

$$\begin{aligned}
2^2 &= 2 \cdot 2 = 4 \\
2^4 &= \left(2^2\right)^2 = 4 \cdot 4 = 16 \\
2^8 &= \left(2^4\right)^2 = 16 \cdot 16 = 256
\end{aligned}$$

In general, using the method:

$$a^2 = a \cdot a, a^3 = a^2 \cdot a, a^4 = a^3 \cdot a, \ldots, a^n = a^{n-1} \cdot a$$

requires $n - 1$ multiplications to compute a^n.

On the other hand if $n = 2^k$ then we can compute a^n by successive squaring with only k multiplications:

$$
\begin{aligned}
a^2 &= a \cdot a \\
a^{2^2} &= \left(a^2\right)^2 = a^2 \cdot a^2 \\
a^{2^3} &= \left(a^{2^2}\right)^2 = a^{2^2} \cdot a^{2^2} \\
&\vdots \\
a^{2^k} &= \left(a^{2^{k-1}}\right)^2 = a^{2^{k-1}} \cdot a^{2^{k-1}}
\end{aligned}
$$

Note that the fact that

$$2^k = \left(2^{k-1}\right) 2 = 2^{k-1} + 2^{k-1}$$

together with the Laws of Exponents:

$$\left(a^n\right)^m = a^{nm}$$

and

$$a^n \cdot a^m = a^{n+m}$$

is what makes this method work. Note that if $n = 2^k$ then k is generally a lot smaller than $n - 1$. For example,

$$1024 = 2^{10}$$

and 10 is quite a bit smaller than 1023.

If n is not a power of 2 we can use the following method to compute a^n.

The Binary Method for Exponentiation. Let n be a positive integer. Let x be any real number. This is a method for computing x^n.

Step 1. Find the binary representation

$$n = [a_r, a_{r-1}, \ldots, a_0]_2$$

for n.

Step 2. Compute the powers

$$x^2, x^{2^2}, x^{2^3}, \ldots, x^{2^r}$$

by successive squaring as shown above.

Step 3. Compute the product

$$x^n = x^{a_r 2^r} \cdot x^{a_{r-1} 2^{r-1}} \cdots x^{a_1 2} \cdot x^{a_0}.$$

[Note each a_i is 0 or 1, so all needed factors were obtained in Step 2.]

Example 26.1. Let's compute 3^{15}. Note that $15 = 2^3 + 2^2 + 2 + 1 = [1,1,1,1]_2$. So this takes care of Step 1. For Step 2, we note that

$$\begin{aligned} 3^2 &= 3 \cdot 3 = 9 \\ 3^{2^2} &= 9 \cdot 9 = 81 \\ 3^{2^3} &= 81 \cdot 81 = 6561 \end{aligned}$$

So $3^{15} = 3^{2^3} \cdot 3^{2^2} \cdot 3^2 \cdot 3^1$. For this we need 3 multiplications:

$$\begin{aligned} 3 \cdot 3^2 &= 3 \cdot 9 = 27 \\ \left(3 \cdot 3^2\right) \cdot 3^{2^2} &= 27 \cdot 81 = 2187 \\ \left(3 \cdot 3^2 \cdot 3^{2^2}\right) 3^{2^3} &= 2187 \cdot 6561 = 14348907 \end{aligned}$$

So we have

$$3^{15} = 14348907.$$

Note that we have used just 6 multiplications, which is less than the 14 it would take if we used the naive method. Let's not forget that some additional effort was needed to compute the binary representation of 15, but not much.

Theorem 26.1. *Computing x^n using the binary method requires $\lfloor \log_2(n) \rfloor$ applications of the Division Algorithm and at most $2\lfloor \log_2(n) \rfloor$ multiplications.*

Proof. If $n = [a_r, \ldots, a_0]_2$, $a_r = 1$, then $n = 2^r + \cdots + a_1 2 + a_0$. Hence

$$(*) \qquad 2^r \leq n \leq 2^r + 2^{r-1} + \cdots + 2 + 1 = 2^{r-1} - 1 < 2^{r+1}.$$

Since $\log_2(2^x) = x$ and when $0 < a < b$ we have $\log_2(a) < \log_2(b)$, we have from $(*)$ that

$$\log_2(2^r) \leq \log_2(n) < \log_2\left(2^{r+1}\right)$$

or

$$r \leq \log_2(n) < r + 1.$$

Hence $r = \lfloor \log_2(n) \rfloor$. Note that r is the number of times we need to apply the Division Algorithm to obtain the binary representation $n = [a_r, \ldots, a_0]_2$, $a_r = 1$. To compute the powers $x, x^2, x^{2^2}, \ldots, x^{2^r}$ by successive squaring requires $r = \lfloor \log_2(n) \rfloor$ multiplications and similarly to compute the product

$$x^{2^r} \cdot x^{a_{r-1}2^{r-1}} \cdots x^{a_1 2} \cdot x^{a_0}$$

requires r multiplicatons. So after obtaining the binary representation we need at most $2r = 2\lfloor \log_2(n) \rfloor$ multiplications. $\square$

Use of a calculator to compute $\log_2(x)$: To find $\log_2(x)$ one may use the formula

$$\log_2(x) = \frac{1}{\ln(2)} \ln(x)$$

or

$$\log_2(x) \approx \left[\frac{1}{(0.69314718)}\right] \ln(x)$$

where $\ln(x)$ is the natural logarithm of x. For small values of x it is sometimes faster to use the fact that $r = \lfloor \log_2(x) \rfloor$ is equivalent to

$$2^r \leq x < 2^{r+1},$$

that is, r is the largest positive integer such that $2^r \leq x$. The Maple command for $\log_2(x)$ is `log[2](x)`.

Note that if we count an application of the Division Algorithm and a multiplication as the same, the above tells us that we need at most $3\lfloor \log_2(n) \rfloor$ operations to compute x^n. So, for example, if $n = 10^6$, then it is easy to see that $3\lfloor \log_2(n) \rfloor = 57$. So we may compute $x^{1{,}000{,}000}$ with only 57 operations.

Exercise 26.1. Calculate $3\lfloor \log_2(n) \rfloor$ for $n = 2,000,000$.

Exercise 26.2. Use the binary method to compute 2^{25}.

Exercise 26.3. Approximately how many operations would be required to compute 2^n when $n = 10^{100}$? Explain.

Exercise 26.4. Note that 6 multiplications are used to compute 3^{15} using the binary method. Show that one can compute 3^{15} with fewer than 6 multiplications. [You will have to experiment.]

Computing $a^n \bmod m$. We use the binary method for exponentiation with the added trick that after every multiplication we reduce modulo m, that is, we divide by m and take the remainder. This keeps the products from getting too big.

Example 26.2. We compute $3^{15} \bmod 10$:

$$\begin{aligned} 3^2 &= 3 \cdot 3 = 9 \equiv 9 \pmod{10} \\ 3^4 &= 9 \cdot 9 = 81 \equiv 1 \pmod{10} \\ 3^8 &\equiv 1 \cdot 1 \equiv 1 \equiv 1 \pmod{10} \\ \therefore 3^{15} &= 3^8 \cdot 3^4 \cdot 3^2 \cdot 3^1 \equiv 1 \cdot 1 \cdot 9 \cdot 3 = 27 \equiv 7 \pmod{10}. \end{aligned}$$

Note that $3^{15} \equiv 7 \pmod{10}$ implies that $3^{15} \bmod 10 = 7$. [Recall that on page 109 we calculated that $3^{15} = 14348907$ which is clearly congruent to 7 mod 10, but the multiplications were not so easy.]

Example 26.3. Let's find $2^{644} \bmod 645$. It is easy to see that

$$644 = [1, 0, 1, 0, 0, 0, 0, 1, 0, 0]_2$$

That is, $644 = 2^9 + 2^7 + 2^2 = 512 + 128 + 4$. Now by successive squaring and reducing modulo 645 we get

$$\begin{aligned} 2^2 &= 2 \cdot 2 = 4 \equiv 4 \pmod{645} \\ 2^4 &\equiv 4 \cdot 4 = 16 \equiv 16 \pmod{645} \\ 2^8 &\equiv 16 \cdot 16 = 256 \equiv 256 \pmod{645} \\ 2^{16} &\equiv 256 \cdot 256 = 65,536 \equiv 391 \pmod{645} \\ 2^{32} &\equiv 391 \cdot 391 = 152,881 \equiv 16 \pmod{645} \\ 2^{64} &\equiv 16 \cdot 16 = 256 \equiv 256 \pmod{645} \\ 2^{128} &\equiv 256 \cdot 256 = 65,536 \equiv 391 \pmod{645} \\ 2^{256} &\equiv 391 \cdot 391 = 152,881 \equiv 16 \pmod{645} \\ 2^{512} &\equiv 16 \cdot 16 = 256 \equiv 256 \pmod{645}. \end{aligned}$$

Now

$$2^{644} = 2^{512} \cdot 2^{128} \cdot 2^4,$$

hence

$$2^{644} \equiv 256 \cdot 391 \cdot 16 \pmod{645}.$$

So

$$256 \cdot 391 = 100099 \equiv 121 \pmod{645}$$

and

$$121 \cdot 16 = 1936 \equiv 1 \pmod{645}$$

so we have $2^{644} \equiv 1 \pmod{645}$. Hence $2^{644} \bmod 645 = 1$.

Exercise 26.5. Calculate $2^{513} \bmod 10$.

Exercise 26.6. Calculate $2^{517} \bmod 100$.

Exercise 26.7. If you multiplied out 2^{517}, how many decimal digits would you obtain? [See Exercise 4.3 on page 14.]

Exercise 26.8. Note that on page 96 we calculated $1234^{7865435} \bmod 11$ with very few multiplications. Why can we not use that method to compute $1234^{7865435} \bmod 12$?

Chapter 27

The RSA Scheme

In this chapter we discuss the basis of the so-called **RSA scheme**. This is the most important example of a *public key cryptographic scheme*. The RSA scheme is due to R. Rivest, A. Shamir and L. Adelman [1] and was discovered by them in 1977. We show how to implement it in more detail later using Maple. Here we give the number-theoretic underpinning of the scheme.

We assume that the message we wish to send has been converted to an integer in the set $J_m = \{0, 1, 2, \ldots, m-1\}$ where m is some positive integer to be determined. Generally this is a large integer. We will require two functions:

$$E : J_m \to J_m \qquad \text{(E for } \textit{encipher}\text{)}$$

and

$$D : J_m \to J_m \qquad \text{(D for } \textit{decipher}\text{)}.$$

To be able to use D to decipher what E has enciphered we need to have $D(E(x)) = x$ for all $x \in J_m$. To show how m, E, and D are chosen we first prove a lemma:

Lemma 27.1. *Let p and q be any two distinct primes and let $m = pq$. Let e and d be any two positive integers which are inverses of each other modulo $\phi(m)$. Then*

$$x^{ed} \equiv x \pmod{m}$$

for all x.

[1] A copy of the paper "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" may be downloaded from http://citeseer.nj.nec.com/rivest78method.html

Proof. By Theorem 22.6, $\phi(m) = (p-1)(q-1)$. Since $ed \equiv 1 \pmod{\phi(m)}$ we have $ed - 1 = k\phi(m) = k(p-1)(q-1)$ for some k. Note $k > 0$ unless $ed = 1$ in which case the theorem is obvious. So we have

$$(*) \qquad ed = k\phi(m) + 1 = k(p-1)(q-1) + 1$$

for some $k > 0$.

Now by Fermat's Little Theorem, if $\gcd(x,p) = 1$ we have $x^{p-1} \equiv 1 \pmod{p}$ and raising both sides of the congruence to the power $(q-1)k$ we obtain:

$$x^{(p-1)(q-1)k} \equiv 1 \pmod{p}$$

and multiplying both sides by x we have

$$x^{(p-1)(q-1)k+1} \equiv x \pmod{p}$$

That is, by $(*)$

$$(**) \qquad x^{ed} \equiv x \pmod{p}.$$

Now we proved $(**)$ when $\gcd(x,p) = 1$, but if $\gcd(x,p) = p$ it is obvious since then $x \equiv 0 \pmod{p}$. So in all cases $(**)$ holds. A similar argument proves that for all x

$$x^{ed} \equiv x \pmod{q}.$$

So by Exercise 15.11, page 63, we have since $\gcd(p,q) = 1$

$$x^{ed} \equiv x \pmod{m}$$

for all x. □

Theorem 27.1. *Let $J_m = \{0, 1, 2, \ldots, m-1\}$ and define $E : J_m \to J_m$ by*

$$E(x) = x^e \bmod m$$

and $D : J_m \to J_m$ by

$$D(x) = x^d \bmod m.$$

Then E and D are inverses of each other if m, e and d are as in Lemma 27.1.

Proof. It suffices to show that $D(E(x)) = x$ for all $x \in J_m$. Let $x \in J_m$ and let $E(x) = x^e \bmod m = r_1$. Also let $D(r_1) = r_1^d \bmod m = r_2$. We must show that $r_2 = x$. Since $x^e \bmod m = r_1$ we know that

$$x^e \equiv r_1 \pmod{m}.$$

Hence $x^{ed} \equiv r_1^d \pmod{m}$. We also know that

$$r_1^d \equiv r_2 \pmod{m}.$$

Hence $x^{ed} \equiv r_2 \pmod{m}$. By Lemma 27.1 $x^{ed} \equiv x \pmod{m}$ so we have

$$x \equiv r_2 \pmod{m}.$$

Since both x and r_2 are in J_m we have by Exercise 15.5 that $x = r_2$. This completes the proof. □

More details on the use of the RSA scheme will be given in the Maple worksheets which are available from the course website which may be reached from my home page: `http://www.math.usf.edu/~eclark`.

Appendix A

Rings and Groups

The material in this appendix is optional reading. However, for the sake of completeness we state here the definition of a *ring* and the definition of a *group*. If you are interested in learning more you might take the course *Elementary Abstract Algebra*. Having had this course should make it a little easier to understand the ideas in abstract algebra and vice versa.

For more details you may download the free book **Elementary Abstract Algebra** from my homepage:

```
http://www.math.usf.edu/~eclark
```

Alternatively, look in almost any book whose title contains the words *Abstract Algebra* or *Modern Algebra*. Look for one with *Introductory* or *Elementary* in the title.

Definition A.1. A **ring** is an ordered triple $(R, +, \cdot)$ where R is a set and $+$ and $\cdot$ are binary operations on R satisfying the following properties:

A1 $a + (b + c) = (a + b) + c$ for all a, b, c in R.

A2 $a + b = b + a$ for all a, b in R.

A3 There is an element $0 \in R$ satisfying $a + 0 = a$ for all a in R.

A4 For every $a \in R$ there is an element $b \in R$ such that $a + b = 0$.

M1 $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all a, b, c in R.

D1 $a \cdot (b + c) = a \cdot b + a \cdot c$ for all a, b, c in R.

D2 $(b+c) \cdot a = b \cdot a + c \cdot a$ for all a, b, c in R.

Thus, to describe a ring one must specify three things:

1. a set,
2. a binary operation on the set called multiplication,
3. a binary operation on the set called addition.

Then, one must verify that the properties above are satisfied.

Example A.1. Here are some examples of rings. The two binary operations $+$ and $\cdot$ are in each case the ones that you are familiar with.

1. $(\mathbb{R}, +, \cdot)$–the ring of real numbers.
2. $(\mathbb{Q}, +, \cdot)$–the ring of rational numbers.
3. $(\mathbb{Z}, +, \cdot)$–the ring of integers.
4. $(\mathbb{Z}_n, +, \cdot)$–the ring of integers modulo n.
5. $(M_n(\mathbb{R}), +, \cdot)$–the ring of all $n \times n$ matrices over $\mathbb{R}$.

Definition A.2. A **group** is an ordered pair $(G, *)$ where G is a set and $*$ is a binary operation on G satisfying the following properties

1. $x * (y * z) = (x * y) * z$ for all x, y, z in G.
2. There is an element $e \in G$ satisfying $e * x = x$ and $x * e = x$ for all x in G.
3. For each element x in G there is an element y in G satisfying $x * y = e$ and $y * x = e$.

Definition A.3. A group $(G, *)$ is said to be **Abelian** if $x * y = y * x$ for all $x, y \in G$.

Thus, to describe a group one must specify two things:

1. a set, and
2. a binary operation on the set.

Then, one must verify that the binary operation is associative, that there is an identity in the set, and that every element in the set has an inverse.

Example A.2. Here are some examples of groups. The binary operations are in each case the ones that you are familiar with.

1. $(\mathbb{Z}, +)$ is a group with identity 0. The inverse of $x \in \mathbb{Z}$ is $-x$.

2. $(\mathbb{Q}, +)$ is a group with identity 0. The inverse of $x \in \mathbb{Q}$ is $-x$.

3. $(\mathbb{R}, +)$ is a group with identity 0. The inverse of $x \in \mathbb{R}$ is $-x$.

4. $(\mathbb{Q} - \{0\}, \cdot)$ is a group with identity 1. The inverse of $x \in \mathbb{Q} - \{0\}$ is x^{-1}.

5. $(\mathbb{R} - \{0\}, \cdot)$ is a group with identity 1. The inverse of $x \in \mathbb{R} - \{0\}$ is x^{-1}.

6. $(\mathbb{Z}_n, +)$ is a group with identity 0. The inverse of $x \in \mathbb{Z}_n$ is $n - x$ if $x \neq 0$, the inverse of 0 is 0.

7. $(U_n, \cdot)$ is a group with identity $[1]$. The inverse of $[a] \in U_n$ was shown to exist in Chapter 22.

8. $(\mathbb{R}^n, +)$ where $+$ is vector addition. The identity is the zero vector $(0, 0, \ldots, 0)$ and the inverse of the vector $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ is the vector $-\mathbf{x} = (-x_1, -x_2, \ldots, -x_n)$.

9. $(M_n(\mathbb{R}), +)$. This is the group of all $n \times n$ matrices over $\mathbb{R}$ and $+$ is matrix addition.

Bibliography

[1] Tom Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York-Heidelberg, 1976.

[2] Chris Caldwell, *The Primes Pages*, `http://www.utm.edu/research/primes/`

[3] W. Edwin Clark, *Number Theory Links*, `http://www.math.usf.edu/~eclark/numtheory_links.html`

[4] Earl Fife and Larry Husch, *Number Theory (Mathematics Archives*, `http://archives.math.utk.edu/topics/numberTheory.html`

[5] Ronald Graham, Donald Knuth, and Oren Patashnik, *Concrete Mathematics*, Addison-Wesley, 1994.

[6] Donald Knuth *The Art of Computer Programming*, Vols I and II, Addison-Wesley, 1997.

[7] The Math Forum, *Number Theory Sites* `http://mathforum.org/library/topics/number_theory/`

[8] Oystein Ore, *Number Theory and its History*, Dover Publications, 1988.

[9] Carl Pomerance and Richard Crandall, *Prime Numbers – A Computational Perspective*, Springer -Verlag, 2001.

[10] Kenneth A. Rosen, *Elementary Number Theory*, (Fourth Edition), Addison-Wesley, 2000.

[11] Eric Weisstein, *World of Mathematics –Number Theory Section*, `http://mathworld.wolfram.com/topics/NumberTheory.html`