12 A Glimpse of Number theory: Exploring the integers[13]

The most familiar mathematical objects are the integers, and *number theory* is the field of mathematics that studies the integers. Despite the apparent simplicity of the integers, number theory is an enormous and complex subject with many unsolved mysteries. Here are two examples.

Twin primes. A pair of primes that differ by two, such as 3 and 5 or 17 and 19 are called *twin primes*. One of the most famous unsolved puzzles in mathematics is the *twin prime conjecture* which asserts that there are infinitely many twin prime pairs. Despite centuries of study, mathematicians still don't know whether this conjecture is correct.

Are there odd perfect numbers? An integer is said to be *perfect* if the sum of its proper divisors (the positive divisors less than itself) is the number itself. For example, 6 is perfect since 6=3+2+1 and 28 is perfect since 28=14+7+4+2+1. (See Exercise 12.16.) Are there any odd perfect numbers?

Exercise 12.1. A *prime triplet* is a sequence of $n, n+2, n+4$ that are all prime. For example 3,5,7 is a prime triplet. Prove that there are no other prime triplets.

12.1 Solving a linear Diophantine Equation

Many problems in number theory deal with finding solutions to an equation, or to a system of equations, where the variables are only allowed to take on integer values. If the equation only involves polynomial functions of the variables, such an equation is called a *Diophantine equation*.

Example 12.1. Consider the equation $x^2 + y^2 = z^2$. If we require x, y and z to be integers we get a Diophantine equation. The solutions to this equation are called *Pythagorean triples*.

Exercise 12.2. Prove that for any two integers m and n, $x = m^2-n^2$, $y = 2mn$ and $z = m^2+n^2$ is a Pythagorean triple.

Example 12.2. Consider the equation $x^4 + y^4 = z^4$. There are trivial integer solutions, where either $x = 0$ or $y = 0$ (in which case the other two numbers are either equal, or one is the negative of the other). Are there any nontrivial solutions (where none of the numbers is 0)? Remarkably, it turns out that there are no such solutions. In fact, one can consider equations of the form $x^k + y^k = z^k$ where k is a positive integer. If $k = 1$ the equation has many non-trivial solutions, and if $k = 2$ solutions are Pythagorean triples. A very famous theorem of Andrew Wiles says that when $k \geq 3$ the only solutions are the trivial ones where x or y is 0. This theorem was first proposed by the French mathematician Pierre de Fermat in 1637, and was not proved until the mid 1990's.

[13]Version 11/10/16.

In this section we investigate the problem of solving a single *linear Diophantine Equation*

Definition 12.1. Let $a_1, \ldots, a_k$ be a list of integers and b be an integer and let $x_1, \ldots, x_k$ be variables. The equation $a_1x_1 + \ldots + a_kx_k$ is a *linear equation* in the k variables $x_1, \ldots, x_k$. If we require that the variables only take integer values, then the equation is a *linear Diophantine equation.*

Example 12.3.
1. The equations $6x = 18$ and $6x = 31$ are one variable linear Diophantine equations. The first has exactly one solution $x = 3$ while the second has no solution.
2. The equation $5x + 8y = 11$ is a linear Diophantine equation. A solution to this equation is $x = 7$, $y = -3$.
3. Does the linear Diophantine equation $6x + 15y = 20$ have a solution?

We are interested in the following questions:

Question 12.3.
1. Is there an easy way to tell whether a Linear Diophantine equation has a solution of not?
2. If the equation does have a solution is there an easy way to find one?
3. If the equation has a solution, how can we describe all of the solutions?

We will answer the first two questions, and give a partial answer to the third. Let's start with the first question. The simplest case is the case of equations with one variable. If we have the equation $ax = b$ then the only possible solution is b/a. If b/a is an integer, then this is the unique solution to the Diophantine equation. If this is not an integer, then the Diophantine euqation has no solutions.

Proposition 12.1. . *Let a and b be arbitrary integers. The linear Diophantine equation $ax = b$ has exactly one solution if a is a divisor of b and has no solutions if a is not a divisor of b.*

Exercise 12.4. Write a careful proof of Proposition 12.1.

Next, let's consider linear Diophantine equations with two variables. Consider the third example in Example 12.3, where you are asked whether $6x + 15y = 20$ has a solution. Notice that 3 is a divisor of both 6 and 15. Therefore whatever integers we choose for x and y, the lefthand side of the equation will be a multiple of 3, while 20 is not a multiple of 3. So it's impossible to find an integer solution to this equation.

For integers a, b and d, we say that d is a *common divisor* of a and b if d is a divisor of a and d is a divisor of b. More generally, for a list $(a_1, \ldots, a_k)$ of integers, and an integer d, we say that d is a *common divisor* of $a_1, \ldots, a_k$ if for each $i \in \{1, \ldots, k\}$ we have d is a divisor of a_i. This argument can be generalized to prove:

Proposition 12.2. *For any integer b and list of integers $(a_1, \ldots, a_k)$, if the equation $a_1x_1 + \cdots + a_kx_k = b$ has a solution with $x_1, \ldots, x_k$ integers, then every common divisor of $a_1, \ldots, a_k$ is a divisor of b.*

Exercise 12.5. Prove Proposition 12.2.

Proposition 12.2 gives a *necessary condition* on $a_1, a_2, \ldots, a_k$and c that must be satisfied for $a_1x_1 + \cdots a_kx_k = b$ to have an integer solution. However, we don't know yet whether that requirement is *sufficient*, which leads to the following question:

Question 12.6. If $a_1, \ldots, a_k$ and b are integers and every common divisor of $a_1, \ldots, a_k$ is also a divisor of b does this imply that the equation $a_1x_1 + \cdots a_kx_k = b$ has an integer solution?

As we will see this question has an affirmative answer. We need some additional definitions.

Definition 12.2. Suppose $a_1, \ldots, a_k$ are integers.

Greatest common divisor. The *greatest common divisor* of $a_1, \ldots, a_k$, denoted $\gcd(a_1, \ldots, a_k)$ is the largest integer that is a divisor of every one of the a_i.

Least common multiple. The *least common multiple* of $a_1, \ldots, a_k$ denoted $\text{lcm}(a_1, \ldots, a_k)$ is the smallest positive integer that is a multiple of every one of the a_i.

Relatively prime. Two integers a and b are said to be *relatively prime* if $\gcd(a, b) = 1$ (so a and b have no common divisor larger than 1). The list $(a_1, \ldots, a_k)$ is a *list of relatively prime integers* if $\gcd(a_i, a_j) = 1$ for all $i \neq j$.

Proposition 12.3. *For any two positive integers a and b, $\gcd(a, b) \times lcm(a, b) = a \times b$.*

Exercise 12.7. Prove Proposition 12.3. (Use the definition of lcm and gcd, and don't use the fact that every integer can be factored uniquely into prime factors.)

Theorem 12.4. *For any nonempty list of positive integers $(a_1, \ldots, a_k)$ and for any positive integer b, the following are equivalent:*

1. *The equation $a_1x_1 + \cdots + a_kx_k = b$ has an all integer solution.*
2. *Every common divisor of $a_1, \ldots, a_k$ is a divisor of b.*
3. *The greatest common divisor of $a_1, \ldots, a_k$ is a divisor of b.*

The proof goes by proving (1) implies (2), (2) implies (3), and (3) implies (1). The proof of (1) implies (2) and (2) implies (3) are easy and left as exercises.

Exercise 12.8. Prove (1) implies (2) and (2) implies (3) for Theorem 12.4.

The hard part is the proof that (3) implies (1). The proof of this will introduce some important new ideas. The first big idea is to change the way we're looking at the problem.

Definition 12.3. For the list $(a_1, \ldots, a_k)$ of integers, we define $S(a_1, \ldots, a_k)$ to be the set of all integers that can be expressed in the form $a_1x_1 + \ldots + a_kx_k$ where $x_1 \ldots, x_s$ are all integers. In set notation $S(a_1, \ldots, a_k) = \{a_1x_1 + \ldots + a_kx_k : x_1, x_2, \ldots, x_k \in \mathbb{Z}\}$.

Example 12.4. We can define $S(m)$ where m is a single integer. In this case, the definition tells us that $S(m)$ is the set of all multiples of m. In particular, $S(0) = \{0\}$.

The question of whether $a_1x_1 + \cdots + a_kx_k = b$ has an integer solution can be restated as: does b belongs to $S(a_1, \ldots, a_k)$? To investiage this question, we will study *the entire set* $S(a_1, \ldots, a_k)$. This seems like we are making the problem harder. However, it turns out that by studying the entire set $S(a_1, \ldots, a_k)$ we will discover that this set has a very simple structure, and once we understand the structure it will be easy to tell whether any particular number b is in the set.

So we explore the set $S(a_1, \ldots, a_k)$ and discover some properties. We start with some simple properties:

Proposition 12.5. *For any integers $a_1, \ldots, a_k$, the numbers $a_1, \ldots, a_k$ and 0 are members of $S(a_1, \ldots, a_k)$.*

Exercise 12.9. Prove Proposition 12.5.

Next we get to some more interesting properties of $S(a_1, \ldots, a_k)$. To state these properties we need some additional definitions.

Definition 12.4. For a subset T of $\mathbb{Z}$ we say:

- T is *closed under addition* if for any $r, s \in T$ we have $r + s \in T$.
- T is *closed under multiplication by* $\mathbb{Z}$ if for any $r \in T$ and $n \in \mathbb{Z}$ we have $nr \in T$.
- T is an *integer ideal* if it is nonempty, closed under addition and closed under multilplication by $\mathbb{Z}$.

Proposition 12.6. *For any integers $a_1, \ldots, a_k$, the set $S(a_1, \ldots, a_k)$ is an integer ideal.*

Exercise 12.10. Prove Proposition 12.6.

In particular, the set $S(0) = \{0\}$ is an ideal, called the *zero ideal*.

So now we know that $S(a_1, \ldots, a_k)$ is an integer ideal. Our next step is a big one. We will show that *every integer ideal is a very simple set*. Recall from Example 12.4 that $S(m)$ is the set of multiples of m.

Theorem 12.7. *For every integer ideal T, there is a nonnegative integer m such that $T = S(m)$.*

This type of theorem is called a *structure theorem*. It says that even though the definition of ideal is somewhat complicated and mysterious, every integer ideal T actually has a very orderly structure.

Proof. Suppose T is an arbitrary integer ideal. We will show that there is an integer m so that $T = S(m)$.

Let's observe first that T must contain 0: Since T is nonempty it contains some integer we'll call t, and by closure under multiplication, $0 \times t = 0$ is in T.

Now we consider two cases: (1) $T = \{0\}$ (T is the zero ideal) and (2) $T \neq \{0\}$ (T is a non-zero ideal).

Case 1. $T = \{0\}$. Then $T = S(0)$.

Case 2. $T \neq \{0\}$. Our goal is to show that there is a positive integer m such that $T = S(m)$.

[**Comment**: *How are we going to give instructions to find m? Imagine that what we are trying to prove is true. Then T consists of all multiples of some positive number m. In this case the positive members of T would be $m, 2m, 3m$, etc. and m is the smallest positive member of T. So this suggests an idea. Even though we don't know that T has the right form, let's pick m to be the smallest positive member of T and try to show that $T = S(m)$.*]

We consider the set $T_{>0}$ consisting of members of T that are positive. We claim $T_{>0}$ is nonempty. Since T is nonempty and not equal to $\{0\}$, it must contain a nonzero member, we'll call t. By closure under multiplication, $-t$ is also in T. One of the numbers t and $-t$ is in $T_{>0}$.

Since $T_{>0}$ is a nonempty subset of positive integers, the well-ordering principle implies that $T_{>0}$ has a smallest member, which we'll call m. Our goal now is to show that $T = S(m)$. To do this we will show $S(m) \subseteq T$ and $T \subseteq S(m)$.

The proof that $S(m) \subseteq T$ is left as an exercise.

Exercise 12.11. For any ideal T and for any $d \in T$, $S(d) \subseteq T$.

The more interesting part is to show that $T \subseteq S(m)$. Suppose t is an arbitrary member of T. We must show that t is a multiple of m. By the quotient-remainder theorem (Theorem 10.14) there are integers q and r with $r \in \{0, \ldots, m-1\}$ such that $t - qm = r$. We will now show that $r = 0$, which implies that $t \in S(m)$. Since $m \in T$ and T is closed under multiplication, we have $-qm$ is in T. Since T is closed under addition $t + (-qm) = t - qm = r$ belongs to T. Now $r \in \{0, \ldots, m-1\} \cap T$ implies $r < m$, and since m is the smallest positive member of T, r can't be a positive integer. Therefore $r = 0$. Therefore $t = qm$ and $t \in S(m)$. □

We are now ready to prove that (3) implies (1) in Theorem 12.4. Recall that $a_1, \ldots, a_k$ are arbitrary positive integers. Suppose that $d = \gcd(a_1, \ldots, a_k)$.

We must show that $S(a_1, \ldots, a_k) = S(d)$. Since $S(a_1, \ldots, a_k)$ is an ideal, Theorem 12.7 implies that there is an integer we'll call m such that $S(a_1, \ldots, a_k) = S(m)$. So we will show $m = d$. To do this we'll show $m \geq d$ and $m \leq d$.

First we show that $m \geq d$. Since d is a divisor of each of the a_i, it is a divisor of any number of the form $a_1x_1 + \cdots + a_kx_k$ where $x_1, \ldots, x_k$ are integers and so d is a divisor of every member of $S(a_1, \ldots, a_m)$. In particular d is a divisor of m and since d and m are positive, $d \leq m$.

Next we show $m \leq d$. By Proposition 12.5, $a_1, \ldots, a_k$ all belong to $S(a_1, \ldots, a_k)$ and since this equals $S(m)$ we have that each a_i is a multiple of m, so m is a common divisor of $a_1, \ldots, a_m$, so $m \leq d$.

Since $d \leq m$ and $m \leq d$ we have $m = d$ and so $S(a_1, \ldots, a_m) = S(d)$ as required to prove the theorem.

□.

The following Corollary is a useful restatement of Theorem 12.4.

Corollary 12.8. *For any integers $a_1, \ldots, a_k$, there are integers $b_1, \ldots, b_k$ such that $a_1b_1 + \cdots + a_kb_k = \gcd(a_1, \ldots, a_k)$.*

Exercise 12.12. Prove Corollary 12.8

Corollary 12.9. *Suppose $m_1, \ldots, m_k$ are integers.*

1. *If d is a common divisor of $m_1, \ldots, m_k$ then d is a divisor of $\gcd(m_1, \ldots, m_k)$.*
2. *If m is a common multiple of $m_1, \ldots, m_k$ then m is a multiple of $lcm(m_1, \ldots, m_k)$.*

Exercise 12.13. Prove Corollary 12.9. (Hint: use induction on k. For the second part, the result of Exercise 12.7 is useful.)

As an application of Corollary 12.8 we will use it to answer a new question:

Question 12.14. Suppose r is a prime number, and $(b_1, \ldots, b_s)$ is a list of integers. If r is not a divisor of any of the b_i, is it possible that r is a divisor of the product?

The following theorem, which is known as Euclid's lemma, shows that the answer to this question is no.

Theorem 12.10. *(Euclid's lemma) For any prime number r and any list of integers $(b_1, \ldots, b_s)$ if r is a divisor of the product $b_1b_2 \ldots b_s$ then there is an index $i \in \{1, \ldots, s\}$ such that r is a divisor of b_i.*

Proof. Suppose that r is an arbitrary prime number and $(b_1, \ldots, b_s)$ is an arbitrary list of integers. We will prove the result by induction on the length s of the list $(b_1, \ldots, b_s)$. By induction we may assume that for any list $(e_1, \ldots, e_t)$ of integers with $t < s$, if r is a divisor of the product then r divides at least one of the e_i. [**Comment**:*The prime r is fixed throughout the proof.*]

We consider two cases, depending on whether $s = 1$, $s = 2$ or $s > 1$.

Case 1. Assume $s = 1$. Then the list is (b_1) and the hypothesis is that r is a divisor of b_1 which is the same as the conclusion.

Case 2. Assume $s = 2$. Then r is a divisor of $b_1 \times b_2$. Assume for contradiction that r is not a divisor of either b_1 or b_2. Since r is prime and r is not a divisor of b_1, $\gcd(r, b_1) = 1$. We will show that $\gcd(b_1b_2, r) = 1$ which will contradict that r is a divisor of b_1b_2. To show that $\gcd(b_1b_2, r) = 1$ we will find integers v and w so that $vb_1b_2 + wr = 1$, which by Proposition 12.2 implies that b_1b_2 and r have no common divisor bigger than 1.

By Corollary 12.8 there are integers we'll call c_1 and d_1 so that $c_1r + d_1b_1 = 1$, and there are integers we'll c_2 and d_2 so that $c_2r + d_2b_2 = 1$. Rewriting these equations we have $d_1b_1 = 1 - c_1r$ and $d_2b_2 = 1 - c_2r$. Multiplying these two equations together gives $d_1d_2b_1b_2 = 1 - (c_1 + c_2 - r)r$, which is equivalent to $d_1d_2b_1b_2 + (c_1 + c_2 - r)r = 1$. So we've found two integers $v = d_1d_2$ and

$w = c_1 + c_2 - r$ so that $vb_1b_2 + wr = 1$. By Theorem **??**, b_1b_2 and r have no common divisor greater than 1, contradicting that r is a divisor of b_1b_2.

Case 3. Assume $s \geq 2$. Let $c = b_2 \times \cdots \times b_s$. Then (b_1, c) is a list of length 2 such that r is a divisor of b_1c so by Case 2, r divides b_1 or r divides c. If r divides b_1 we have what we want. If r divides c then we have that r is a divisor of the product of the list $(b_2, \ldots, b_{s-1})$. Since this list has length $s - 1$, by the induction hypothesis, r is a divisor of at least one of the numbers $b_2, \ldots, b_s$, as required. □

We will apply this Theorem in the next two sections to prove additional results in number theory.

12.2 The fundamental theorem of arithmetic

Recall that a *factorization* of a positive integer n is a list of positive integers, all greater than 1, whose product is n; the list may just be the single entry list (n). Recall that a prime number is an integer greater than 1 that has no divisors other than itself and 1. A *prime factorization* of n is a factorization of n consisting entirely of primes. For example, $(2, 2, 2, 3, 5)$ is a prime factorization of 120. There are two obvious questions to ask about prime factorizations:

Question 12.15. 1. Does every positive integer greater than 1 have a prime factorization?

2. Does any integer have more than one prime factorization?

In middle school or high school you probably learned about prime factorizations, and had practice finding the prime factorization of a number. From your experience, you can probably guess that the answer to the first question is yes: Every positive integer greater than 1 has a prime factorization. You may recall that this statement was proved earlier as Theorem **??**.

The answer to the second question is no since $(2, 3, 3)$ and $(3, 3, 2)$ are two different prime factorizations of 18. Of course, one of these lists is just a *rearrangement* of the other: every prime appears the same number of times in each list, but in a different order. So we modify the second part of Question 12.15 to ask: can an integer have two prime factorizations that are not rearrangements of each other?

This answer to this question is provided by the following theorem, which is so important that it is called the *fundamental theorem of arithimetic*.

Theorem 12.11. *(Fundamental theorem of arithmetic) For any integer $n \geq 2$, the prime factorization of n is unique up to rearrangement, which means that any two prime factorizations of n must be rearrangements of each other.*

Proof. Suppose n is an arbitrary integer greater than 1. We already proved that n has at least one factorization, so now we show that for any two factorizations, one must be a rearrangement of the other. We use mathematical induction. By induction we may assume that for any integer k such that $k > 1$ and $k < n$, any two factorizations of k must be rearrangements of each other.

Suppose that $(p_1, \ldots, p_k)$ and $(q_1, \ldots, q_m)$ are arbitrary prime factorization of n. We now show that at least one of the primes in the list $(q_1, \ldots, q_m)$ is equal to p_1. Since $n = q_1 \ldots q_m$

and p_1 is a divisor of n, we have $p_1|q_1 \cdots q_m$. By Euclid's lemma 12.10, there is a $j \in \{1, \ldots, m\}$ such that p_i is a divisor of q_j. Since q_j is prime and $p_1 > 1$ we must have $p_1 = q_j$.

So p_1 appears on both lists (possibly more than once). Let P be the list obtained by removing p_1 from the first list and let Q be the list obtained by removing q_j from the second. We then have two lists of primes that both are factorizations of the number $n' = n/p_1$. We also have $n' > 1$ since by the case assumption n is not prime. So $n' > 1$ and $n' < n$ so by the induction hypothesis P and Q must be rearrangements of the other. Since $(p_1, \ldots, p_k)$ is obtained by adding p_1 to the list P and $(q_1, \ldots, q_m)$ is obtained by adding $q_j = p_1$ to the list Q we have that $(p_1, \ldots, p_k)$ is a rearrangement of $(q_1, \ldots, q_m)$ as required. □

Exercise 12.16. Recall that a number is perfect if the sum of its proper divisors is the number itself. (A *proper divisor* of the positive integer n is a positive divisor less than n.) Prove that if n is a positive integer such that $2^n - 1$ is prime then $2^{n-1}(2^n - 1)$ is perfect. Use this result to find a perfect number bigger than 30.

12.3 Systems of congruences in one variable

Let's start with a sample problem:

Question 12.17. Is there a number n such that $n \equiv_3 1$ and $n \equiv_4 2$ and $n \equiv_5 4$? If so find such a number.

Here we have three separate requirements on n, the first says that $n - 1$ is divisible by 3, the second says $n - 2$ is divisible by 4 and the third says $n - 4$ is divisible by 5.

In this section, we consider problems with this general form.

Definition 12.5. A *system of congruences* in the variable n is a sequence of constraints on n that is described by a list of pairs of integers $(b_1, m_1), (b_2, m_2), \ldots, (b_k, m_k)$ where each m_i is positive. The constraints are:

$$
\begin{aligned}
n &\equiv_{m_1} b_1 && (1)\\
n &\equiv_{m_2} b_2 && (2)\\
&\cdot && (3)\\
&\cdot && (4)\\
&\cdot && (5)\\
n &\equiv_{m_k} b_k. && (6)
\end{aligned}
$$

- We refer to m_i as the *modulus* of the ith constraint and b_i is the *remainder* of the ith contraint.
- We refer to the list $m_1, \ldots, m_k$ as the *list of moduli*, and to the list $b_1, \ldots, b_k$ as the *list of remainders* of the system.

The *solution set* $S(b_1, b_2, \ldots, b_k; m_1, \ldots, m_k)$ is the set of integers n that satisfy (1).

Given a list of pairs of integers $(b_1, m_1), \ldots, (b_k, m_k)$, there are some natural questions:

Question 12.18. 1. Does the associated system of congruences have a solution? (Is $S(b_1, \ldots, b_k; m_1, \ldots, m_k)$ nonempty?)

2. If the system has a solution, what is a method to find it?

3. Is there an easy way to describe the set $S(b_1, \ldots, b_k; m_1, \ldots, m_k)$?

In this section we'll investigate these questions. We will think about the problem in the following way: Think of $m_1, \ldots, m_k$ as fixed. For each choice of the list of remainders $b_1, \ldots, b_k$ we get a solution set (which might be empty). As we vary $b_1, \ldots, b_k$ we want to understand how the solution set changes. The following fact says that we can relate the solutions of different lists of remainders. First we need a definition:

Definition 12.6 (Sum of lists)**.** If $a = (a_1, \ldots, a_k)$ and $b = (b_1, \ldots, b_k)$ are lists then $a + b$ is defined to be the list $(a_1 + b_1, \ldots, a_k + b_k)$.

Lemma 12.12. *Suppose $m_1, \ldots, m_k$ is a list of positive integers.*

1. *Suppose that $a_1, \ldots, a_k$ and $b_1, \ldots, b_k$ are two lists of integers. Suppose that n belongs to $S(a_1, \ldots, a_k; m_1, \ldots, m_k)$ and r belongs to $S(b_1, \ldots, b_k; m_1, \ldots, m_k)$. Then $n + r$ belongs to $S(a_1 + b_1, \ldots, a_k + b_k; m_1, \ldots, m_k)$.*

2. *Suppose we have t lists of possible remainders*

$$b^1 = (b_1^1, \ldots, b_k^1), b^2 = (b_1^2, \ldots, b * 2_k), \ldots, (b_1^t, \ldots, b_k^t)$$

and that $n_1, \ldots, n_t$ are integers such that for each i, $n_i \in S(b_1^i, \ldots, b_k^i; m_1, \ldots, m_k)$. Let $c = (c_1, \ldots, c_k)$ be the sum of the lists $b^1 + \cdots + b^t$. Prove that $n_1 + \ldots, n_t \in S(c_1, \ldots, c_k; m_1, \ldots, m_k)$

Exercise 12.19. Prove Lemma 12.12. When proving the second part, use induction on t, and notice that the case $t = 2$ is equivalent to the first part.

Now, let's consider the case that all of the remainders are 0. This is referred to as a system of *homogeneous congruences*. This case has a simple solution:

Proposition 12.13. *For any list of positive integers $m_1, \ldots, m_k$, the set $S(0, \ldots, 0; m_1, \ldots, m_k)$ of all solutions to the system of congruences $n \equiv_{m_i} 0$ for each $i \in \{1, \ldots, k\}$ is equal to the set of multiples of $lcm(m_1, \ldots, m_k)$.*

Exercise 12.20. Prove Proposition 12.13. (Hint: Corollary 12.9 is helpful.)

Now let's consider the case of general congruences where the remainders are not all 0. In this case, finding a solution is not so easy. However, it turns out that if we are able to find one solution, then there is an easy way to determine the entire set of possible solutions!

Proposition 12.14. *Suppose $(b_1, m_1), \ldots, (b_k, m_k)$ is a list of pairs of integers and n_0 is a member of $S(b_1, \ldots, b_k; m_1, \ldots, m_k)$. Then for all integers n, n is a solution if and only if $n - n_0$ is a multiple of $lcm(m_1, \ldots, m_k)$.*

Exercise 12.21. Prove Proposition 12.14.

Armed with Proposition 12.14, we only need to find a single solution to a system of congruences and then we know all solutions. So we focus on the first two parts of Question 12.18. We will not answer these questions for all possible systems, but we will give a solution in the special case of *relatively prime moduli*, which means that any two moduli in the system have greatest common divisor equal to 1. For example, the system in Question 12.17 has moduli 3,4 and 5, which are relatively prime. In the case of relatively prime moduli we'll show that there is always a solution, and we'll show how to find one. This theorem is often called the Chinese Remainder Theorem, because the earliest known discovery of it was in the 3rd century C.E. by the Chinese mathematician Sunzi.

Theorem 12.15. *Every system of congruences with relatively prime moduli has a solution.*

We will give two proofs of this theorem. The proofs are quite different and each proof is interesting. The proofs both require the assumption that the moduli are relatively prime. Here are the facts that we need about lists of relatively prime integers.

Proposition 12.16. *Let $r_1, \ldots, r_j$ be a list of positive integers that are relatively prime. Then:*

1. *$lcm(r_1, \ldots, r_j) = r_1 \times \cdots \times r_j$.*
2. *For any number s that is relatively prime to each r_j, s is also relatively prime to the product $r_1 \times \cdots \times r_j$*

Exercise 12.22. Prove Proposition 12.16. (Hint: For the first part use induction on j. The case $j = 1$ is trivial. Prove the case $j = 2$ using Proposition 12.3. Use the induction hypothesis to prove the case $j \geq 3$. For the second part, use Euclid's Lemma (Theorem 12.10)).

Proof 1 of Theorem 12.15. Suppose $m_1, \ldots, m_k$ are positive integers and $b_1, \ldots, b_k$ are integers. We want to show that there exists a solution to (1). We will do this by showing how to construct a solution.

Here's our strategy: We saw above that if the b_i are all equal to 0, then its easy to find a solution. Suppose for the moment we could find a solution in the case that all but one of the b_i are 0. Define k lists, $d^1, d^2, \ldots, d^k$ where the list d^i has ith entry b_i and all other entries 0. Notice that b is the sum of the lists $d^1, \ldots, d^k$. Suppose for each i, we manage to find a solution n_i to the congruences when the remainder list is d^i. Then by Lemma 12.12 we have that $n_1 + \cdots + n_k$ is a solution to the congruences with remainder list $(b_1, \ldots, b_k)$.

So now we only have to show how to find a solution n_i for the congruence with remainder list d^i whose only nonzero entry is $d^i_i = b_i$. For the moment, let's consider the problem of finding a number that satisfies all of the requirements*except possibly for the* $n \equiv_{m_i} b_i$. Then we have $k - 1$ requirements all having remainder 0. Define N_i to be the product of all of the

moduli except for m_i. By Proposition 12.16, part 1, since the m_i are relatively prime, N_i is also equal to the lcm of all of the moduli except for m_i. By Proposition 12.13, any multiple of N_i satisfies all congruences except the ith. So now we just need to find a multiple of N_i that satisfies the ith requirement, since that number will satisfy all of the requirements. We want to find a number r_i so that $r_i N_i - a_i$ is a multiple of m_i, which means that we want to find integers r_i and s_i so that $r_i N_i + s_i m_i = a_i$. Now, since m_i is relatively prime to m_j for every $j \neq i$, by Proposition 12.16, Part 2, m_i is relatively prime to M_i, so by Corollary 12.8 there are integers we'll call b and c so that $bm_i + cM_i = 1$. Multiplying both sides by a_i we have $(a_i b)m_i + (a_i c)M_i = a_i$. So we let $n_i a_i c M_i - a_i$ which is divisible by m_i and is a multiple of every other m_i.

Now, following the above strategy we define $n = \sum_{i=1}^{k} n_i$, which is a solution to the original system of congruences. □

Now we'll move on to the other proof. This proof is quite different from the previous. Notice that the theorem we're proving is a "universal-existential" assertion, it says that "*for all* system of congruences having relatively prime moduli, *there exists* a solution". The first proof followed the usual pattern for a universal-existential assertionL An arbitrary system of congruences was introduced. We then had to show that there exists a solution, so we gave instructions for building a solution. The second proof will not follow this pattern. We will manage to show that there exists a solution, not by giving instructions for building a solution, but by a completely new method.

Proof 2 of Theorem 12.15. Suppose $m_1, \ldots, m_k$ are positive integers and $b_1, \ldots, b_k$ are integers. We want to show that there exists an integer n such that for each $i \in \{1, \ldots, k\}$, $n \equiv_{m_i} b_i$.

We now do a few things to modify our goal. For $i \in \{1, \ldots, k\}$ define the set S_i to be $\{0, \ldots, m_i - 1$. For each $i \in \{1, \ldots, k\}$, let c_i be the remainder when b_i is divided by m_i. Observe that $c_i \in S_i$. Since $b_i \equiv_{m_i} c_i$ we can reformulate our goal as: Does the system of congruences $n \equiv_{m_i} c_i$ for $i \in \{1, \ldots, k\}$ have a solution?

Next we define a function r that maps each integer n to a list of k numbers, where the ith entry of the list is denoted $r_i(n)$, so $r(n) = (r_1(n), \ldots, r_k(n))$. The function $r_i(n)$ is defined to be the remainder when you divide n by m_i, so that $r_i(n) \in A_i$. So the range of the function r is a subset of $S_1 \times \cdots \times S_k$. We can restate what we want to show in terms of the function r: we want to show that $(c_1, \ldots, c_k)$ is in the range of r, which means that there is an integer n such that $r(n) = (c_1, \ldots, c_k)$. Such an n is a solution to the system of congruences.

Usually, the way we show that a particular object is in the range of a function is to construct a member of the domain that maps to that object. Here we'll use a very different technique. We will show that the range of r is the entire set $S_1 \times \cdots \times S_k$. Since $(c_1, \ldots, c_k) \in S_1 \times \cdots \times S_k$ we will conclude that $(c_1, \ldots, c_k) \in \mathbf{Range}(r)$.

Observe that the size of the set $S_1 \times \cdots \times S_k$ is $|S_1| \times \cdots \times |S_k| = m_1 \times \cdots \times m_k$. Let us call this last number N. Consider the function q obtained by restricting the function r to the with domain $\{0, \ldots, N-1\}$. Call this function q, so that $q : \{0, \ldots, N-1\} \longrightarrow S_1 \times \cdots \times S_k$. Notice that both of these sets have the same size N. We will prove that q is onto, which obviously implies that r is onto.

To prove that q is onto we'll use the following fact.

> If A and B are finite sets of the same size, then any one-to-one map from A to B is also onto.

This fact is intuitively obvious and is stated as Proposition **??**. This fact is useful because it gives us a completely different way to prove that the function q is onto: since the domain and codomain of q are finite sets that the same size, it is enough to show that q is one-to-one. So we do this.

Suppose s and t are integers in $\{0, \ldots, N-1\}$. Assume $q(s) = q(t)$. We must show $s = t$. Assume without loss of generality that $s \geq t$ and let $w = s - t$. Then $q(w)$ is equal to $(0, \ldots, 0)$ so w is a solution to the homogenous system of congruences $n \equiv_{m_i} 0$ for all $i \in \{1, \ldots, k\}$. By Proposition 12.13, we know that w is a multiple of $\text{lcm}(m_1, \ldots, m_k)$, which is equal to N by Proposition 12.16, Part 1. But $w \in \{0, \ldots, N-1\}$ so $w = 0$ and therefore $s = t$ as required to prove that q is one-to-one. Therefore q is also onto! □

12.4 Decimal representations of integers

Our culture represents integers using the base 10 representation. In this representation we have 10 symbols called digits, which are 0,1,2,3,4,5,6,7,8,9 and which stand for the first 10 nonnegative integers. If $d_0, d_1, \ldots, d_k$ is a sequence of digits then when we write them in reverse order $d_k d_{k-1} \ldots, d_0$ (without commas) this means the number $\sum_{i=0}^{k} d_i 10^i$. This is called the *base 10* or *decimal representation* of an integer. When representing a positive integer, we insist the highest order digit be nonzero, so we don't allow 00353, and instead write 353. There are two key questions:

- Can every positive integer be represented in this way.
- Is the decimal representation of every positive integer unique?

Of course, our experience tells us that these things seem to be true. Now we'll prove them.

Theorem 12.17. *For every positive integer n, there is a unique sequence of digits $d_0, \ldots, d_k$ that gives the decimal representation of n.*

We'll prove this in two parts. First we prove that every positive integer n has a decimal representation. Then we'll prove that n has at most one decimal representation. In the proof of the first part, we'll use induction, but it will not be enough just to apply the induction hypothesis to $n - 1$.

Proof. Suppose n is an arbitrary positive integer. We'll show that n has a unique decimal representation. First we prove that n has a decimal representation. Then we'll prove that any two such representations must be the same.

We start by showing that n has a decimal representation.

Case 1. If $n \leq 9$ then n has a single digit decimal representation.

Case 2. Assume $n \geq 10$. We divide into case depending on whether $10|n$ or not.
Subcase 2a. Assume n is divisible by 10. Let $m = n/10$. By the induction assumption, there are numbers $a_0, \ldots, a_t$ such that $m = \sum_{i=0}^{t} a_i 10^i$. Then $n = 10 * m$. Define $c_0, \ldots, c_{t+1}$ by $c_0 = 0$ and for $1 \leq j \leq t+1$, $c_j = a_{j-1}$. Then $n = \sum_{i=0}^{t} a_i 10^{i+1} = \sum_{j=1}^{t+1} a_{j-1} 10^j = \sum_{j=0}^{t+1} c_j 10^j$.
Subcase 2a. Assume 10 is not a divisor of n. Apply the induction hypothesis to $n-1$ to get a decimal representation $b_j b_{j-1} \ldots b_0$ for $n-1$. We claim that $b_0 < 9$. If not then $n-1-9$ is divisible by 10, and so $n-10$ is divisible by 10, contradicting that n is not divisible by 10. Since $b_0 < 9$ we can simply define $c_0 = b_0 + 1$ and $c_j = b_j$ for $j \geq 1$, and then $\sum_{i=0}^{j} c_i 10^i = n$.

This completes the proof that n has a decimal representation. Next we want to prove that the representation is unique.

Lemma 12.18. *For any positive integer j and for any sequence $a_0, \ldots, a_{j-1}$ of digits we have $10^j > \sum_{i=0}^{j-1} a_i 10^i$.*

Proof. Suppose j is a positive integer and that $a_0, \ldots, a_{j-1}$ is a sequence of digits. We have $\sum_{i=0}^{j-1} a_i 10^i \leq \sum_{i=0}^{j-1} 9 \times 10^i$, since $a_i \leq 9$ for each i. Now using the formula for geometric series, Proposition 11.6, we have $\sum_{i=0}^{j-1} 9(10^i) = 9(10^j - 1)/9 = 10^j - 1$, which is an upper bound on the sum. □

Now given the lemma, suppose that $d_j d_{j-1} \ldots d_0$ and $c_k c_{k-1} \ldots c_0$ are both decimal representations of n. Note that by the requirements on decimal representations $d_j \neq 0$ and $c_k \neq 0$. We need to show that these representations are the same. So we have to show $j = k$ and that two sequences have the same digits. We claim that $j = k$. By the lemma, $n = \sum_{i=0}^{j} d_i 10^i < 10^{j+1}$ and also $n \geq d_j 10^j \geq 10^j$. Similarly $n < 10^{k+1}$ and $n \geq 10^k$. So $10^{k+1} > n \geq 10^j$ which implies $k \geq j$ and $10^{j+1} > n \geq 10^k$ which implies $j \geq k$. Thus $j = k$.

Suppose for contradiction that $d_j \ldots d_0$ and $c_j \ldots c_0$ are different. Let h be the largest index such that $c_h \neq d_h$. We may assume that $d_h > c_h$ (the other case is similar.) Then:

$$\begin{aligned}
\sum_{i=0}^{j} d_i 10^i - \sum_{i=0}^{j} c_i 10^i &= \sum_{i=0}^{j} (d_i - c_i) 10^i \\
&\geq \sum_{i=0}^{h} (d_i - c_i) 10^i \\
&= (d_h - c_h) 10^h + \sum_{i=0}^{h-1} (d_i - c_i) 10^i \\
&\geq 10^h - \sum_{i=0}^{h-1} c_i 10^i.
\end{aligned}$$

By the lemma, this difference is positive, which contradicts that both of these sequences represent the same number n. □