Chapter 12

More on Prime Numbers

As you are probably beginning to appreciate, the prime numbers are fundamental to our understanding of the integers. In this chapter we will discuss a few basic results concerning the primes, and also hint at the vast array of questions, some solved, some unsolved, in current research into prime numbers.

The first few primes are

$$2,3,5,7,11,13,17,19,23,29,31,37,41,43,\ldots$$

It is quite simple to carry on a long way with this list, particularly if you have a computer at hand. How would you do this? The easiest way is probably to test each successive integer n for primality, by checking, for each prime $p \leq \sqrt{n}$, whether p divides n (such primes p will of course already be in your list). If none of these primes p divides n, then n is prime — see Exercise 2 at the end of the chapter. Some more sophisticated methods for primality testing will be discussed at the end of Chapter 14.

Probably the first and most basic question to ask is: Does this list ever stop? In other words, is there a *largest* prime number, or does the list of primes go on forever? The answer is provided by the following famous theorem of Euclid (300 BC).

THEOREM 12.1
There are infinitely many prime numbers.

PROOF This is one of the classic proofs by contradiction. Assume the result is false – that is, there are only finitely many primes. This means that we can make a finite list

$$p_1, p_2, p_3, \ldots, p_n$$

of *all* the prime numbers. Now define a positive integer

$$N = p_1 p_2 p_3 \ldots p_n + 1 \ .$$

By Proposition 8.1, N is equal to a product of primes, say $N = q_1 \dots q_r$ with all q_i prime. As q_1 is prime, it belongs to the above list of all primes, so $q_1 = p_i$ for some i.

Now q_1 divides N, and hence p_i divides N. Also p_i divides $p_1 p_2 \dots p_n$, which is equal to $N-1$. Thus, p_i divides both N and $N-1$. But this implies that p_i divides the difference between these numbers, namely 1. This is a contradiction. ∎

Theorem 12.1 is of course not the end of the story about the primes — it is really the beginning. A natural question to ask that flows from the theorem is: What *proportion* of all positive integers are prime? On the face of it this question makes no sense, as the integers and the primes are both infinite sets. But one can make a sensible question by asking

Given a positive integer n, how many of the numbers $1, 2, 3, \dots, n$ are prime?

Is there any reason to expect to be able to answer this question? On the face of it, no. If you stare at a long list of primes, you will see that the sequence is very irregular, and it is very difficult to see any pattern at all in it. (See, for example, Exercise 6 at the end of the chapter.) Why on earth should there then be a nice formula for the number of primes up to n?

The amazing thing is that there *is* such a formula, albeit an "asymptotic" one. (I will explain this word later.) The great Gauss, by calculating a lot with lists of primes (and also by having a lot of brilliant thoughts), formed the incredible conjecture (i.e., informed guess) that the number of primes up to n should be pretty close to the formula

$$\frac{n}{\log_e n}.$$

To understand this a little, compare the number of primes up to 10^6 (namely, 78498) with the value of $\frac{10^6}{\log 10^6}$ (namely, 72382.4). The *difference* between these two numbers, about 6000, appears to be quite large; but their *ratio* is 1.085, quite close to 1. It was on the ratio, rather than the difference, that Gauss concentrated his mind: his conjecture was that the ratio of the number of primes up to n and the expression $\frac{n}{\log_e n}$ should get closer and closer to 1 as n gets larger and larger. (Formally, this ratio *tends to* 1 *as n tends to infinity*.)

Gauss did not actually manage to prove his conjecture. The world had to wait until 1896, when a Frenchman, Hadamard, and a Belgian, de la Vallée-Poussin, both produced proofs of what is now known as the Prime Number Theorem:

THEOREM 12.2

For a positive integer n, let $\pi(n)$ be the number of primes up to n. Then the ratio of $\pi(n)$ and $\frac{n}{\log_e n}$ tends to 1 as n tends to infinity (i.e., the ratio can be made as close as we like to 1 provided n is large enough).

The proof of this result uses some quite sophisticated tools of analysis. Nevertheless, if you are lucky you might get the chance to see a proof in an undergraduate course later in your studies — in other words, it is not *that* difficult!

You should not think that every question about the primes can be answered (if not by you, then by some expert or other). On the contrary, many basic questions about the primes are unsolved to this day, despite being studied for many years. Let me finish this chapter by mentioning a couple of the most famous such problems.

The Goldbach conjecture If you do some calculations, or program your computer, you will find that any reasonably small even positive integer greater than 2 can be expressed as a sum of two primes. For example,

$$10 = 7+3,\ 50 = 43+7,\ 100 = 97+3,\ 8000 = 3943+4057$$

and so on. Based on this evidence, it seems reasonable to conjecture that *every* even positive integer is the sum of two primes. This is the Goldbach conjecture, and it is unsolved to this day.

The twin prime conjecture If p and $p+2$ are both prime numbers, we call them *twin primes*. For example, here are some twin primes:

$$3,5;\ 5,7;\ 11,13;\ 71,73;\ 1997,1999.$$

If you stare at a list of prime numbers, you will find many pairs of twin primes, getting larger and larger. One feels that there should be infinitely many twin primes, and indeed, that statement is known as the twin prime conjecture. Can one prove the twin prime conjecture using a proof like Euclid's in Theorem 12.1? Unfortunately not — indeed, no one has come up with any sort of proof, and the conjecture remains unsolved to this day.

Exercises for Chapter 12

1. Prove Liebeck's *triplet prime conjecture*: the only triplet of primes of the form $p, p+2, p+4$ is $\{3,5,7\}$.

2. Let n be an integer with $n \geq 2$. Suppose that for every prime $p \leq \sqrt{n}$, p does not divide n. Prove that n is prime.

   Is 221 prime? Is 223 prime?

3. For a positive integer n, define $\phi(n)$ to be the number of positive integers $a < n$ such that $\text{hcf}(a,n) = 1$. (For example, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$.)

   Work out $\phi(n)$ for $n = 5, 6, \ldots, 10$.

   If p is a prime, show that $\phi(p) = p - 1$ and, more generally, that $\phi(p^r) = p^r - p^{r-1}$.

4. Use the idea of the proof of Euclid's Theorem 12.1 to prove that there are infinitely many primes of the form $4k+3$ (where k is an integer).

5. There has been quite a bit of work over the years on trying to find a nice formula that takes many prime values. For example, x^2+x+41 is prime for all integers x such that $-40 \leq x < 40$. (You may like to check this!) However:

   Find an integer x coprime to 41 such that x^2+x+41 is not prime.

6. On his release from prison, critic Ivor Smallbrain rushes out to see the latest film, *Prime and Prejudice*. During the film Ivor attempts to think of ten consecutive positive integers, none of which is prime. He fails.

   Help Ivor by showing that if $N = 11! + 2$, then none of the numbers $N, N+1, N+2, \ldots, N+9$ is prime.

   More generally, show that for any $n \in \mathbb{N}$ there is a sequence of n consecutive positive integers, none of which is prime. (Hence, there are arbitrarily large "gaps" in the sequence of primes.)

Chapter 13

Congruence of Integers

In this chapter we introduce another method for studying the integers, called congruence. Let us go straight into the definition.

DEFINITION *Let m be a positive integer. For $a, b \in \mathbb{Z}$, if m divides $b-a$ we write $a \equiv b \mod m$ and say a is congruent to b modulo m.*

For example,

$$5 \equiv 1 \mod 2, \quad 12 \equiv 17 \mod 5, \quad 91 \equiv -17 \mod 12, \quad 531 \not\equiv 0 \mod 4 .$$

PROPOSITION 13.1
Every integer is congruent to exactly one of the numbers $0, 1, 2, \ldots, m-1$ modulo m.

PROOF Let $x \in \mathbb{Z}$. By Proposition 10.1, there are integers q, r such that

$$x = qm + r \quad \text{with} \quad 0 \leq r < m .$$

Then $x - r = qm$, so m divides $x-r$, and hence by the above definition, $x \equiv r \mod m$. Since r is one of the numbers $0, 1, 2, \ldots, m-1$, the proposition follows. ∎

Example 13.1

(1) Every integer is congruent to 0 or 1 modulo 2. Indeed, all even integers are congruent to 0 modulo 2 and all odd integers to 1 modulo 2.

(2) Every integer is congruent to 0, 1, 2 or 3 modulo 4. More specifically, every even integer is congruent to 0 or 2 modulo 4 and every odd integer to 1 or 3 modulo 4.

(3) My clock is now showing the time as 2:00a.m. What time will it be showing in 4803 hours? Since $4803 \equiv 3 \mod 24$, it will be showing a

time 3 hours later than the current time, namely 5:00a.m. (But I hope I will not be awake to see it.)

The next result will be quite useful for our later work involving manipulation of congruences.

PROPOSITION 13.2
Let m be a positive integer. The following are true, for all $a,b,c \in \mathbb{Z}$:
(1) $a \equiv a \bmod m$,
(2) *if* $a \equiv b \bmod m$ *then* $b \equiv a \bmod m$,
(3) *if* $a \equiv b \bmod m$ *and* $b \equiv c \bmod m$, *then* $a \equiv c \bmod m$.

PROOF (1) Since $m|0$ we have $m|a-a$, and hence $a \equiv a \bmod m$.
(2) If $a \equiv b \bmod m$ then $m|b-a$, so $m|a-b$, and hence $b \equiv a \bmod m$.
(3) If $a \equiv b \bmod m$ and $b \equiv c \bmod m$, then $m|b-a$ and $m|c-b$; say $b-a=km, c-b=lm$. Then $c-a=(k+l)m$, so $m|c-a$, and hence $a \equiv c \bmod m$. ∎

Arithmetic with Congruences

Congruence is a notation that conveniently records various divisibility properties of integers. This notation comes into its own when we do arithmetic with congruences, as we show is possible in the next two results. The first shows that congruences modulo m can be added and multiplied.

PROPOSITION 13.3
Suppose $a \equiv b \bmod m$ and $c \equiv d \bmod m$. Then

$$a+c \equiv b+d \bmod m \quad \text{and} \quad ac \equiv bd \bmod m\ .$$

PROOF We are given that $m|b-a$ and $m|d-c$. Say $b-a=km$ and $d-c=lm$, where $k,l \in \mathbb{Z}$. Then

$$(b+d)-(a+c)=(k+l)m$$

and hence $a+c \equiv b+d \bmod m$. And

$$bd-ac=(a+km)(c+lm)-ac=m(al+ck+klm),$$

which implies that $ac \equiv bd \bmod m$. ∎

PROPOSITION 13.4
If $a \equiv b \bmod m$, and n is a positive integer, then

$$a^n \equiv b^n \bmod m\ .$$

PROOF We prove this by induction. Let $P(n)$ be the statement of the proposition. Then $P(1)$ is obviously true.
Now suppose $P(n)$ is true, so $a^n \equiv b^n \bmod m$. As $a \equiv b \bmod m$, we can use Proposition 13.3 to multiply these congruences and get $a^{n+1} \equiv b^{n+1} \bmod m$, which is $P(n+1)$. Hence, $P(n)$ is true for all n by induction. ∎

These results give us some powerful methods for using congruences, as we shall now attempt to demonstrate with a few examples.

Example 13.2
Find the remainder r (between 0 and 6) that we get when we divide 6^{82} by 7.

Answer We start with the congruence $6 \equiv -1 \bmod 7$. By Proposition 13.4, we can raise this to the power 82, to get $6^{82} \equiv (-1)^{82} \bmod 7$, hence $6^{82} \equiv 1 \bmod 7$. This means that 7 divides $6^{82}-1$; hence $6^{82}=7q+1$ for some $q \in \mathbb{Z}$, and so the remainder is 1.

Example 13.3
Find the remainder r (between 0 and 12) that we get when we divide 6^{82} by 13.

Answer This is not quite so easy as the previous example. We employ a general method, which involves "successive squaring" of the congruence $6 \equiv 6 \bmod 13$. Squaring once, we get $6^2 \equiv 36 \bmod 13$; since $36 \equiv -3 \bmod 13$, Proposition 13.2(3) gives $6^2 \equiv -3 \bmod 13$. Successive squaring like this yields:

$$\begin{aligned} 6^2 &\equiv -3 \bmod 13\ , \\ 6^4 &\equiv 9 \bmod 13\ , \\ 6^8 &\equiv 3 \bmod 13\ , \\ 6^{16} &\equiv 9 \bmod 13\ , \\ 6^{32} &\equiv 3 \bmod 13\ , \end{aligned}$$

$$6^{64} \equiv 9 \bmod 13 .$$

Now $6^{82} = 6^{64}6^{16}6^2$. Multiplying the above congruences for $6^{64}, 6^{16}$ and 6^2, we get

$$6^{82} \equiv 9 \cdot 9 \cdot (-3) \bmod 13 .$$

Now $9 \cdot (-3) = -27 \equiv -1 \bmod 13$, so $6^{82} \equiv -9 \equiv 4 \bmod 13$. Hence, the required remainder is 4.

The method given in this example is called the *method of successive squares* and always works to yield the congruence of a large power, given some effort. To work out the congruence modulo m of a power x^k of some integer x, express k as a sum of powers of 2 (you might have met this before as "writing k in base 2" or some such phrase) — say $k = 2^{a_1} + \cdots + 2^{a_r}$; then successively square to work out the congruences modulo m of the powers $x^{2^{a_1}}, \ldots, x^{2^{a_r}}$, and multiply these together to obtain the answer.

Sometimes this effort can be reduced with some clever trickery, as in Example 13.2.

Example 13.4

Show that no integer square is congruent to 2 modulo 3. (In other words, the sequence $2, 5, 8, 11, 14, 17, \ldots$ contains no squares.)

Answer Consider an integer square n^2 (where $n \in \mathbb{Z}$). By Proposition 13.1, n is congruent to 0, 1 or 2 modulo 3. If $n \equiv 0 \bmod 3$, then by Proposition 13.4, $n^2 \equiv 0 \bmod 3$; if $n \equiv 1 \bmod 3$, then $n^2 \equiv 1 \bmod 3$; and if $n \equiv 2 \bmod 3$, then $n^2 \equiv 4 \bmod 3$, and hence [using 13.2(3)] $n^2 \equiv 1 \bmod 3$. This shows that integer squares are congruent to 0 or 1 modulo 3.

Example 13.5

Show that every odd integer square is congruent to 1 modulo 4.

Answer This is similar to the previous example. Let n be an odd integer. Then n is congruent to 1 or 3 modulo 4, so n^2 is congruent to 1 or 9 modulo 4, hence to 1 modulo 4.

Example 13.6

The "rule of 3" You may have come across a simple rule for testing whether an integer is divisible by 3: add up its digits, and if the sum is divisible by 3 then the integer is divisible by 3. Here is a quick explanation of why this rule works.

Let n be an integer, with digits $a_r a_{r-1} \ldots a_0$, so

$$n = a_0 + 10a_1 + 10^2 a_2 + \cdots + 10^r a_r .$$

Now $10 \equiv 1 \bmod 3$; hence, by Proposition 13.4, $10^k \equiv 1 \bmod 3$ for any positive integer k. Multiplying this by the congruence $a_k \equiv a_k \bmod 3$ gives $10^k a_k \equiv a_k \bmod 3$. It follows that

$$n \equiv a_0 + a_1 + \cdots + a_r \bmod 3 .$$

Hence, $n \equiv 0 \bmod 3$ if and only if the sum of its digits $a_0 + \cdots + a_r \equiv 0 \bmod 3$. This is the "rule of 3."

The same method proves the "rule of 9": an integer is divisible by 9 if and only if the sum of its digits is divisible by 9. There is also a "rule of 11," which is not quite so obvious: an integer n with digits $a_r \ldots a_1 a_0$ is divisible by 11 if and only if the expression $a_0 - a_1 + a_2 - \cdots + (-1)^r a_r$ is divisible by 11. Proving this is Exercise 4 at the end of the chapter. You will also find other rules in Exercise 5.

Unlike adding and multiplying, we can't always divide congruences modulo m. For example, $10 \equiv 6 \bmod 4$, but we can't divide this by 2 to deduce that $5 \equiv 3 \bmod 4$. However, the next result shows that there are some circumstances in which we can divide congruences.

PROPOSITION 13.5

(1) Let a and m be coprime integers. If $x, y \in \mathbb{Z}$ are such that $xa \equiv ya \bmod m$, then $x \equiv y \bmod m$.

(2) Let p be a prime, and let a be an integer that is not divisible by p. If $x, y \in \mathbb{Z}$ are such that $xa \equiv ya \bmod p$, then $x \equiv y \bmod p$.

PROOF (1) Assume that $xa \equiv ya \bmod m$. Then m divides $xa - ya = (x-y)a$. Since a, m are coprime, Proposition 10.5(a) implies that m divides $x - y$. In other words, $x \equiv y \bmod m$.

Part (2) is immediate from part (1), since if a is not divisible by a prime p, then a and p are coprime. ∎

Congruence Equations

Let m be a positive integer and let $a, b \in \mathbb{Z}$. Consider the equation

$$ax \equiv b \bmod m$$

to be solved for $x \in \mathbb{Z}$. Such an equation is called a linear congruence equation. When does such an equation have a solution?

Example 13.7

(1) Consider the congruence equation

$$4x \equiv 2 \bmod 28 .$$

If $x \in \mathbb{Z}$ is a solution to this, then $4x = 2+28n$ for some integer n, which is impossible since the left-hand side is divisible by 4, whereas the right-hand side is not. So this congruence equation has no solutions.

(2) Now consider the equation

$$13x \equiv 2 \bmod 31 .$$

We shall show that this equation has a solution. Observe that $\text{hcf}(13,31) = 1$; hence, by Proposition 10.3, there are integers s,t such that

$$1 = 13s+31t .$$

Therefore, $13s = 1-31t$, which means that $13s \equiv 1 \bmod 31$. Multiplying this congruence by 2, we get

$$13 \cdot (2s) \equiv 2 \bmod 31 .$$

In other words, $x = 2s$ is a solution to the original congruence equation.

Here is a general result telling us exactly when linear congruence equations have solutions.

PROPOSITION 13.6

The congruence equation

$$ax \equiv b \bmod m$$

has a solution $x \in \mathbb{Z}$ if and only if $\text{hcf}\,(a,m)$ *divides b.*

PROOF Write $d = \text{hcf}(a,m)$. First let us prove the left-to-right implication. So suppose the equation has a solution $x \in \mathbb{Z}$. Then $ax = qm+b$ for some integer q. Since $d|a$ and $d|m$, it follows that $d|b$.

Now for the right-to-left implication. Suppose $d|b$, say $b = kd$. By Proposition 10.3, there are integers s,t such that $d = sa+tm$. Multiplying through by k gives $b = kd = k(sa+tm)$. Hence,

$$aks = b-ktm \equiv b \bmod m .$$

In other words, $x = ks$ is a solution to the congruence equation. ∎

We shall see some different types of congruence equations in the next chapter.

The System $\mathbb{Z}_m$

The properties of congruence modulo m can be encapsulated rather neatly by defining a new system, denoted by $\mathbb{Z}_m$, which we can think of as "the integers modulo m." Before defining this in general, here is an example.

Example 13.8

Take $m = 4$. Let $\mathbb{Z}_4$ be the set consisting of the four integers 0, 1, 2, 3, and define addition and multiplication of any two numbers in $\mathbb{Z}_4$ to be the same as for $\mathbb{Z}$, except that we make sure the answer is again in $\mathbb{Z}_4$ by taking congruences modulo 4. For example, to add 2 and 3 in $\mathbb{Z}_4$, we first note that their sum in $\mathbb{Z}$ is 5; the number in $\mathbb{Z}_4$ that is congruent to 5 modulo 4 is 1, so in $\mathbb{Z}_4$ we define the sum $2+3$ to be 1. Here are some other examples of addition and multiplication in $\mathbb{Z}_4$:

$$1+2 = 3,\ 0+3 = 3,\ 2+2 = 0,\ 3+3 = 2,$$

and

$$0 \times 3 = 0,\ 2 \times 3 = 2,\ 3 \times 3 = 1.$$

The full addition and multiplication tables for $\mathbb{Z}_4$ are as follows:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

In general, for a fixed positive integer m, the system $\mathbb{Z}_m$ is defined in an entirely similar way. We take $\mathbb{Z}_m$ to be the set consisting of the m integers $0,1,2,\ldots,m-1$ and define addition and multiplication of any two numbers in $\mathbb{Z}_m$ to be the same as for $\mathbb{Z}$, except that we make sure the answer is again in $\mathbb{Z}_m$ by taking congruences modulo m. More formally, for $x,y \in \mathbb{Z}_m$, the sum and product of x and y in $\mathbb{Z}_m$ are defined to be the numbers $k,l \in \mathbb{Z}_m$ such that $x+y \equiv k \bmod m$ and $xy \equiv l \bmod m$, respectively. We'll write $x+y = k$ and $xy = l$ in $\mathbb{Z}_m$.

For example, in $\mathbb{Z}_5$ we have $4+4 = 3$; in $\mathbb{Z}_7$ we have $5 \times 3 = 1$; and in any $\mathbb{Z}_m$, we have $(m-1)+(m-2) = m-3$ and $(m-1)(m-2) = 2$.

The system $\mathbb{Z}_m$ is quite a useful one. We can do quite a bit of algebra in it, such as taking powers and solving equations. Here are a few more examples.

Example 13.9

(1) We can define powers of elements of $\mathbb{Z}_m$ in a natural way: for $x \in \mathbb{Z}_m$ and $r \in \mathbb{N}$, the r^{th} power of x in $\mathbb{Z}_m$ is defined to be the number $k \in \mathbb{Z}_m$ such that $x^r \equiv k \bmod m$. For example, in $\mathbb{Z}_5$, we have

$$2^2 = 4,\ 2^3 = 3,\ 2^4 = 1.$$

Examples 13.2 and 13.3 show that in $\mathbb{Z}_7$, we have $6^{82} = 1$, while in $\mathbb{Z}_{13}$, $6^{82} = 4$.

(2) Proposition 13.6 tells us that for $a, b \in \mathbb{Z}_m$, the equation $ax = b$ has a solution for $x \in \mathbb{Z}_m$ if and only if $\text{hcf}(a,m)$ divides b. So, for example, the equation $2x = 7$ has a solution in $\mathbb{Z}_9$ (namely $x = 8$), but not in $\mathbb{Z}_{10}$.

(3) Examples 13.4 and 13.5 show that the quadratic equation $x^2 = 2$ has no solution in $\mathbb{Z}_3$, and $x^2 = 3$ has no solution in $\mathbb{Z}_4$. In general, to see whether an equation in a variable x has a solution in $\mathbb{Z}_m$, unless we can think of anything better we can always just try substituting each of the m possible values for x and seeing if they work. For example, does the equation

$$x^2 + 3x + 4 = 0$$

have a solution in $\mathbb{Z}_5$? Well, if we substitute the five possible values for x into the expression $x^2 + 3x + 4$ and work out the answer in $\mathbb{Z}_5$, here is what we get:

x	0	1	2	3	4
x^2+3x+4	4	3	4	2	2

So the answer is no, there is no solution in $\mathbb{Z}_5$. However, this equation does have solutions in $\mathbb{Z}_{11}$, for example — namely $x = 3$ or 5.

Exercises for Chapter 13

1. (a) Find r with $0 \le r \le 10$ such that $7^{137} \equiv r \bmod 11$.

   (b) Find r with $0 \le r < 645$ such that $2^{81} \equiv r \bmod 645$.

   (c) Find the last two digits of 3^{124} (when expressed in decimal notation).

   (d) Show that there is a multiple of 21 which has 241 as its last three digits.

2. Let p be a prime number and k a positive integer.

   (a) Show that if x is an integer such that $x^2 \equiv x \bmod p$, then $x \equiv 0$ or $1 \bmod p$.

   (b) Show that if x is an integer such that $x^2 \equiv x \bmod p^k$, then $x \equiv 0$ or $1 \bmod p^k$.

3. For each of the following congruence equations, either find a solution $x \in \mathbb{Z}$ or show that no solution exists:

   (a) $99x \equiv 18 \bmod 30$

   (b) $91x \equiv 84 \bmod 143$

   (c) $x^2 \equiv 2 \bmod 5$

   (d) $x^2 + x + 1 \equiv 0 \bmod 5$

   (e) $x^2 + x + 1 \equiv 0 \bmod 7$

   (f) Find all positive integer solutions or show that no solution exists:
   (i) $9x \equiv 144 \pmod{99}$
   (ii) $18x \equiv 30 \pmod{40}$
   (iii) $3x \equiv 2 \pmod{7}$

4. (a) Prove the "rule of 9": an integer is divisible by 9 if and only if the sum of its digits is divisible by 9.

   (b) Prove the "rule of 11" stated in Example 13.6. Use this rule to decide in your head whether the number 82918073579 is divisible by 11.

5. (a) Use the fact that 7 divides 1001 to find your own "rule of 7." Use your rule to work out the remainder when 6005004003002001 is divided by 7.

   (b) 13 also divides 1001. Use this to get a rule of 13 and find the remainder when 6005004003002001 is divided by 13.

   (c) Use the observation that $27 \times 37 = 999$ to work out a rule of 37, and find the remainder when 6005004003002001 is divided by 37.

6. Let p be a prime number, and let a be an integer that is not divisible by p. Prove that the congruence equation $ax \equiv 1 \bmod p$ has a solution $x \in \mathbb{Z}$.

7. Show that every square is congruent to 0, 1 or -1 modulo 5, and is congruent to 0, 1 or 4 modulo 8.

   Suppose n is a positive integer such that both $2n+1$ and $3n+1$ are squares. Prove that n is divisible by 40.

   Find a value of n such that $2n+1$ and $3n+1$ are squares. Can you find another value? (Calculators allowed!)

8. Find $x, y \in \mathbb{Z}_{15}$ such that $xy = 0$ but $x \neq 0, y \neq 0$ (where xy means the product in $\mathbb{Z}_{15}$).

   Find a condition on m such that the equality $xy = 0$ in $\mathbb{Z}_m$ implies that either $x = 0$ or $y = 0$.

9. Let p be a prime and let $a, b \in \mathbb{Z}_p$, with $a \neq 0$ and $b \neq 0$. Prove that the equation $ax = b$ has a solution for $x \in \mathbb{Z}_p$.

10. Construct the addition and multiplication tables for $\mathbb{Z}_6$. Find all solutions in $\mathbb{Z}_6$ of the equation $x^2 + x = 0$.

11. It is Friday, May 6, 2005. Ivor Smallbrain is watching the famous movie *From Here to Infinity*. He is bored, and idly wonders what day of the week it will be on the same date in 1000 years' time (i.e., on May 6, 3005). He decides it will again be a Friday.

    Is Ivor right? And what has this question got to do with congruence?

12. Prove that if $ca \equiv cb \pmod{m}$ and $\gcd(c,m) = d$ then $a \equiv b \pmod{\frac{m}{d}}$

13. Find m in (i) $29 \equiv 7 \pmod{m}$
    (ii) $53 \equiv 0 \pmod{m}$

14. Find (i) $2^{28} \pmod{7}$
    (ii) $3^{65} \pmod{13}$
    (iii) $53^{103} + 103^{53} \pmod{39}$.

Chapter 14

More on Congruence

In this chapter we are going to see some further results about congruence of integers. Most of these are to do with working out the congruence of large powers of an integer modulo some given integer m. I showed you some ways of tackling this kind of question in the last chapter (see Examples 13.2 and 13.3). The first result of this chapter — Fermat's Little Theorem — is a general fact that makes powers rather easy to calculate when m is a prime number. The rest of the chapter consists mainly of applications of this theorem to solving some special types of congruence equations modulo a prime or a product of two primes, and also to the problem of finding large prime numbers using a computer. We'll make heavy use of all this material in the next chapter on secret codes.

Fermat's Little Theorem

This very nifty result was first found by the French mathematician Fermat around 1640. It is called Fermat's Little Theorem to distinguish it from the rather famous "Fermat's Last Theorem," which is somewhat harder to prove (although why the adjective "little" was chosen, rather than "large" or "medium-sized" or "nifty," is not clear to me).

Anyway, here it is.

THEOREM 14.1 (Fermat's Little Theorem)
Let p be a prime number, and let a be an integer that is not divisible by p. Then

$$a^{p-1} \equiv 1 \ mod\ p.$$

For example, applying the theorem with $p = 17$ tells us that $2^{16} \equiv 1 \bmod 17$, that $93^{16} \equiv 1 \bmod 17$, and indeed that $72307892^{16} \equiv 1 \bmod 17$. This makes

congruences of powers modulo 17 fairly painless to calculate. For instance, let's work out 3^{972} modulo 17. Well, we know that $3^{16} \equiv 1 \bmod 17$. Dividing 16 into 972, we get $972 = 16 \cdot 60 + 12$, so

$$3^{972} = (3^{16})^{60} \cdot 3^{12} \equiv (1^{60}) \cdot 3^{12} \bmod 17.$$

So we only need to work out 3^{12} modulo 17. This is easily done using the method of successive squares explained in Example 13.3: we get $3^2 \equiv 9 \bmod 17$, so $3^4 \equiv 9^2 \equiv 13 \bmod 17$, so $3^8 \equiv 13^2 \equiv (-4)^2 \equiv 16 \bmod 17$. Hence

$$3^{972} \equiv 3^{12} \equiv 3^4 \cdot 3^8 \equiv 13 \cdot 16 \equiv 4 \bmod 17.$$

PROOF Here's a proof of Fermat's Little Theorem. For an integer x, we shall write $x \pmod p$ to denote the integer k between 0 and $p-1$ such that $x \equiv k \bmod p$. (So, for example, $17 \pmod 7 = 3$.) Also, for integers $x_1, \ldots, x_k$, we write $x_1, \ldots, x_k \pmod p$ as an abbreviation for the list $x_1 \pmod p, \ldots, x_k \pmod p$. (So for example, the list $17, 32, -1 \pmod 7$ is $3, 4, 6$.)

Now let a, p be as in the theorem. Multiply each of the numbers $1, 2, 3, \ldots, p-1$ by a and take congruences modulo p to get the list

$$a, 2a, 3a, \ldots, (p-1)a \pmod p. \tag{14.1}$$

(For example, if $p = 7$ and $a = 3$, this list is $3, 6, 2, 5, 1, 4$.)

We claim that the list (14.1) consists of the numbers $1, 2, 3, \ldots, p-1$ in some order. To see this, note first that since p does not divide a, none of the numbers in the list is 0. Next, suppose two of the numbers in the list are equal, say $xa \pmod p = ya \pmod p$ (where $1 \leq x, y \leq p-1$). Saying that $xa \pmod p = ya \pmod p$ is the same as saying that $xa \equiv ya \bmod p$. By Proposition 13.5(2), this implies that $x \equiv y \bmod p$, and since x and y are between 1 and $p-1$, this means that $x = y$. This shows that the numbers listed in (14.1) are all different. As there are $p-1$ of them, and none of them is 0, they must be the numbers $1, 2, 3, \ldots, p-1$ in some order.

Now let's multiply together all the numbers in the list (14.1). The result is $a^{p-1} \cdot (p-1)! \pmod p$. Since the numbers in the list are just $1, 2, 3, \ldots p-1$ in some order, this product is also equal to $(p-1)! \pmod p$. In other words, $a^{p-1} \cdot (p-1)! \pmod p = (p-1)! \pmod p$, which means that

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \bmod p.$$

Now p does not divide $(p-1)!$ (since none of the factors $p-1, p-2, \ldots 3, 2$ is divisible by p). Hence Proposition 13.5(2) allows us to cancel $(p-1)!$ in the above congruence equation to deduce that $a^{p-1} \equiv 1 \bmod p$. This completes the proof. ∎

Notice that Fermat's Little Theorem implies that if p is prime, then $a^p \equiv a \bmod p$ for all integers a, regardless of whether a is divisible by p (since if p divides a then obviously $a^p \equiv a \equiv 0 \bmod p$). For a different proof of Fermat's Little Theorem, see Exercise 9 at the end of Chapter 16.

It is possible to use Fermat's Little Theorem to show that a number N is not a prime without actually finding any factors of N. For example, suppose we are trying to test whether the number 943 is prime. One test is to raise some number, say 2, to the power 942 and see whether the answer is congruent to 1 modulo 943; if it's not, then 943 is not a prime by Fermat's Little Theorem. In fact, using the method of successive squares (see Example 13.3) we can calculate that

$$2^{942} \equiv 496 \bmod 943,$$

showing that indeed 943 is not a prime.

Of course, for such a small number as 943 it would be much quicker to test it for primality by simply looking for prime factors less than $\sqrt{943}$. However, for really large numbers the above test can be rather effective. Let's call it the *Fermat test*.

The Fermat test is by no means always successful in detecting the non-primality of a number. For example, you will find that $2^{340} \equiv 1 \bmod 341$, which gives you no information about whether or not 341 is prime. (In fact, it is not prime, since $341 = 11 \cdot 31$.) Indeed, there are some numbers N that are not prime yet satisfy $a^{N-1} \equiv 1 \bmod N$ for all integers a coprime to N, and for these numbers the Fermat test will never detect their non-primality. The smallest such number is 561 (see Exercise 3 at the end of the chapter).

We shall see in the next chapter that it is very important to be able to find very large primes using computers, so finding good primality tests is vital. There are some clever refinements of the Fermat test that work well in practice, and I'll discuss these later in this chapter.

Before moving on to the next section, we note the following result, which is an easy consequence of Fermat's Little Theorem. We'll need this also in the next chapter.

PROPOSITION 14.1

Let p and q be distinct prime numbers, and let a be an integer that is not divisible by p or by q. Then

$$a^{(p-1)(q-1)} \equiv 1 \bmod pq.$$

PROOF By Fermat's Little Theorem we know that $a^{p-1} \equiv 1 \bmod p$. Taking $(q-1)^{th}$ powers of both sides (which we can do by Proposition 13.4), it follows that $a^{(p-1)(q-1)} \equiv 1 \bmod p$. Similarly $a^{q-1} \equiv 1 \bmod q$, and hence also $a^{(q-1)(p-1)} \equiv 1 \bmod q$. Therefore, both p and q divide

$a^{(p-1)(q-1)} - 1$, so pq divides this number (since p and q both appear in its prime factorization). In other words, $a^{(p-1)(q-1)} \equiv 1 \bmod pq$, as required. ∎

Finding k^{th} roots modulo m

We now consider congruence equations of the form

$$x^k \equiv b \bmod m,$$

where m, b and k are given integers and we want to solve for $x \pmod m$. We can regard any such solution x as a k^{th} root of b modulo m, so solving this equation is equivalent to finding k^{th} roots modulo m.

In fact we now have enough theory in place to be able to do this under certain assumptions when m is either a prime or a product of two primes. Let's begin with an example.

Example 14.1
Solve the equation $x^{11} \equiv 5 \bmod 47$.

Answer Let x be a solution, so

$$x^{11} \equiv 5 \bmod 47. \tag{14.2}$$

We also know by Fermat's Little Theorem that

$$x^{46} \equiv 1 \bmod 47. \tag{14.3}$$

The idea is to combine (14.2) and (14.3) in a clever way to find x.

The key is to observe that 11 and 46 are coprime, and so, using Proposition 10.3 and Exercise 2 of Chapter 10, we can find positive integers s, t such that $11s - 46t = 1$. So $11s = 1 + 46t$ and $11s \equiv 1 \bmod 46$. Then

$$x \cdot (x^{46})^t = x^{1+46t} = x^{11s} = (x^{11})^s,$$

and so by (14.2) and (14.3),

$$x \equiv 5^s \bmod 47.$$

In fact, using the Euclidean algorithm we find that $1 = 21 \cdot 11 - 5 \cdot 46$, so we take $s = 21, t = 5$. Using the method of successive squares (see Example 13.3), we see that $5^{21} \equiv 15 \bmod 47$.

This shows that $x \pmod{47} = 15$ is the only possible solution. To check that it really is a solution, work backwards in the above calculation: if $x \equiv 5^s \bmod 47$, then

$$x^{11} \equiv 5^{11s} \equiv 5^{1+46t} \equiv 5 \cdot (5^{46})^t \equiv 5 \bmod 47,$$

so this is indeed a solution.

The general case is no harder than this example. Here it is.

PROPOSITION 14.2
Let p be a prime, and let k be a positive integer coprime to $p-1$. Then
(i) there is a positive integer s such that $sk \equiv 1 \bmod (p-1)$, and
(ii) for any $b \in \mathbb{Z}$ not divisible by p, the congruence equation

$$x^k \equiv b \bmod p$$

has a unique solution for x modulo p. This solution is $x \equiv b^s \bmod p$, where s is as in (i).

PROOF (i) Since k and $p-1$ are coprime, Proposition 10.3 implies that there are integers s, t such that $sk - t(p-1) = 1$. We wish to take s to be positive; we can do this by adding a multiple of $p-1$ to it, provided we add the same multiple of k to t. (Here we are simply observing that $(s + a(p-1))k - (t + ak)(p-1) = 1$ for any a.) We now have $sk = 1 + t(p-1) \equiv 1 \bmod (p-1)$ with s positive, proving (i).

(ii) Suppose that x is a solution to $x^k \equiv b \bmod p$. Since p does not divide b, it does not divide x, so by Fermat's Little Theorem we have $x^{p-1} \equiv 1 \bmod p$. Hence

$$x \equiv x^{1+t(p-1)} \equiv x^{sk} \equiv (x^k)^s \equiv b^s \bmod p.$$

Hence the only possible solution is $x \equiv b^s \bmod p$, and this is indeed a solution, since

$$(b^s)^k \equiv b^{sk} \equiv b^{1+t(p-1)} \equiv b \cdot (b^{p-1})^t \equiv b \bmod p.$$

∎

A simple modification of the proof enables us to find k^{th} roots modulo a product of two primes. Here is the result, which will be crucial to our discussion of secret codes in the next chapter.

PROPOSITION 14.3

Let p,q be distinct primes, and let k be a positive integer coprime to $(p-1)(q-1)$. Then

(i) there is a positive integer s such that $sk \equiv 1 \mod (p-1)(q-1)$, and

(ii) for any $b \in \mathbb{Z}$ not divisible by p or by q, the congruence equation

$$x^k \equiv b \mod pq$$

has a unique solution for x modulo pq. This solution is $x \equiv b^s \mod pq$, where s is as in (i).

PROOF The proof is just like that of the previous proposition, except that at the beginning we find integers s,t such that

$$sk - t(p-1)(q-1) = 1,$$

and at the end we use Proposition 14.1 instead of Fermat's Little Theorem. ∎

Finding Large Primes

In the next chapter I will introduce you to some very clever secret codes that are used every day for the secure transmission of sensitive information. These codes are based on some of the theory of prime numbers and congruence that we have covered already. For practical use of the codes, one of the basic requirements is the ability to find very large prime numbers using a computer — prime numbers with more than 200 digits are required. So here is a brief discussion of how this is done in practice.

The key is to have a good primality test; in other words, given a very large number N on our computer, we want a method that the computer can quickly apply to tell whether this number N is prime or not. We have already seen earlier in this chapter one idea for such a method, based on the Fermat test: using the method of successive squares, test whether $a^{N-1} \equiv 1 \mod N$ for a reasonable number of values of a. If this is false for any of these values a, then N is not prime by Fermat's Little Theorem. However, if it is true for all the tested values of a, then while it is rather likely that N is prime, it is not definite — there are numbers N (such as 561) for which $a^{N-1} \equiv 1 \mod N$ for all integers a coprime to N, yet N is not prime.

However, there is a neat variant of the Fermat test that does work in practice. It is based on the following simple fact.

PROPOSITION 14.4

Let p be a prime. If a is an integer such that $a^2 \equiv 1 \mod p$, then $a \equiv \pm 1 \mod p$.

PROOF Assume that $a^2 \equiv 1 \mod p$. Then p divides a^2-1, which is equal to $(a-1)(a+1)$. Hence, by Proposition 10.5(b), p divides either $a-1$ or $a+1$. In other words, either $a \equiv 1 \mod p$ or $a \equiv -1 \mod p$. ∎

Here then is the variant of the Fermat test known as *Miller's test*. Let N be an odd positive integer to be tested for primality, and let b be a positive integer less than N (known as the *base*). First, test whether $b^{N-1} \equiv 1 \mod N$. If this is false we know that N is not prime, and stop; if it is true, we work out $b^{(N-1)/2} \pmod N$. If this is not $\pm 1 \pmod N$, then N is not prime by Proposition 14.4, and we say that N fails Miller's test with the base b, and stop. If it is $-1 \pmod N$, we say that N passes Miller's test with the base b, and stop. And if it is $1 \pmod N$, then we repeat: work out $b^{(N-1)/4} \pmod N$ (assuming 4 divides $N-1$) – if this is not $\pm 1 \pmod N$, then N is not prime and fails Miller's test; if it is $-1 \pmod N$, N passes Miller's test; and if it is $1 \pmod N$, we repeat, this time working out $b^{(N-1)/8} \pmod N$ (assuming 8 divides $N-1$).

We carry on repeating this process. One of the following three things will happen:

(1) at some point we get a value that is not $\pm 1 \pmod N$;

(2) at some point we get $-1 \pmod N$;

(3) we always get $1 \pmod N$ until we run out of powers of 2 to divide $N-1$ by (in other words, we get $b^{(N-1)/2^i} \equiv 1 \mod N$ for $i = 0, \ldots s$, where $N-1 = 2^s \cdot m$ with m odd).

If (1) happens, we say that N fails Miller's test with the base b, and if (2) or (3) happens, we say that N passes Miller's test with the base b.

Example 14.2

We've seen (or at least I have told you!) that it is impossible to show that 561 is not prime using the Fermat test (since $a^{560} \equiv 1 \mod 561$ for all a coprime to 561). But if you do Miller's test with the base 5, you will find at the first step that $5^{(561-1)/2} = 5^{280} \equiv 67 \mod 561$; hence, 561 fails Miller's test and is not prime.

We know that if N fails Miller's test then it is definitely not prime. But what if N passes the test? Here's the crux: a clever — but not too difficult

— argument shows that if b is chosen at random and N is *not* prime, then the chance that N passes Miller's test with the base b is less than $\frac{1}{4}$. Hence if we do the test with k different bases, the chance N will pass all k tests is less than $(\frac{1}{4})^k$. Taking $k = 100$, say, this chance is $(\frac{1}{4})^{100}$, which is about 10^{-60}, and this is less than the chance that your computer makes an error in its calculations along the way.

To summarise, we now have a powerful, albeit "probabilistic" primality test for a large integer N: pick at random 100 positive integers less than N, and do Miller's test on N with each of these as the base. If N fails any of the tests, it is not prime; and if it passes all of them then N is almost certainly a prime, the chance of getting the answer wrong being less than the chance of a computer error.

For a discussion of this and more powerful tests, see the book by K.H. Rosen listed in the Further Reading at the end of this book.

Exercises for Chapter 14

1. (a) Find $3^{301} \pmod{11}$, $5^{110} \pmod{13}$ and $7^{1388} \pmod{127}$.

   (b) Show that $n^7 - n$ is divisible by 42 for all positive integers n.

2. Let a, b be integers, and let p be a prime not dividing a. Show that the solution of the congruence equation $ax \equiv b \bmod p$ is $x \equiv a^{p-2}b \bmod p$.

   Use this observation to solve the congruence equation $4x \equiv 11 \bmod 19$.

3. Let $N = 561 = 3 \cdot 11 \cdot 17$. Show that $a^{N-1} \equiv 1 \bmod N$ for all integers a coprime to N.

4. Let p be a prime number and k a positive integer.

   (a) Show that if p is odd and x is an integer such that $x^2 \equiv 1 \bmod p^k$, then $x \equiv \pm 1 \bmod p^k$.

   (b) Find the solutions of the congruence equation $x^2 \equiv 1 \bmod 2^k$. (*Hint:* There are different numbers of solutions according to whether $k = 1$, $k = 2$ or $k > 2$.)

5. Show that if p and q are distinct primes, then $p^{q-1} + q^{p-1} \equiv 1 \bmod pq$.

6. The number $(p-1)! \pmod{p}$ came up in our proof of Fermat's Little Theorem, although we didn't need to find it. Calculate $(p-1)! \pmod{p}$ for some small prime numbers p. Find a pattern and make a conjecture.

   Prove your conjecture! (*Hint:* You may find Exercise 6 of Chapter 13 useful.)

7. (a) Solve the congruence equation $x^3 \equiv 2 \bmod 29$.

   (b) Find the 7^{th} root of 12 modulo 143 (i.e., solve $x^7 \equiv 12 \bmod 143$).

   (c) Find the 11^{th} root of 2 modulo 143.

8. Use Miller's test with a few different bases to try to discover whether 2161 is a prime number. Make sure your answer has a chance of at least 98% of being correct.

9. In a late-night showing of the Spanish cult movie *Teorema Poca de Fermat*, critic Ivor Smallbrain is dreaming that the answer to life, the universe and everything is 1387, provided this number is prime. He tries Fermat's test on 1387, then Miller's test, both with the base 2.

   What are the results of Ivor's tests? Has he found the answer to life, the universe and everything?

10. Find the remainder of $13^{133} + 5$ on division by 19.

11. Determine whether or not $11^{204} + 1$ is divisible by 13.

12. use FLT to deduce that $17 \mid (13^{16n+2} + 1)$ for all $n \in \mathbb{Z}^+$