1.3 Congruences

For many problems involving integers, all of the relevant information is contained in the remainders obtained by dividing by some fixed integer n. Since only n different remainders are possible $(0, 1, \ldots, n-1)$, having only a finite number of cases to deal with can lead to considerable simplifications. For small values of n it even becomes feasible to use trial-and-error methods.

Example 1.3.1 (Sums of squares).

> A famous theorem of Lagrange states that every positive integer can be written as sum of four squares. (See the notes at the end of this chapter for a short discussion of this problem.) To illustrate the use of remainders in solving a number theoretic problem, we will show that any positive integer whose remainder is 7 when divided by 8 cannot be written as the sum of three squares. Therefore this theorem of Lagrange is as sharp as possible.
>
> If $n = a^2 + b^2 + c^2$, then when both sides are divided by 8, the remainders must be the same. It will follow from Proposition 1.3.3 that we can compute the remainder of $n = a^2 + b^2 + c^2$ by adding the remainders of a^2, b^2, and c^2 (and subtracting a multiple of 8 if necessary). By the same proposition, we can compute the remainders of a^2, b^2, and c^2 by squaring the remainders of a, b, and c (and subtracting a multiple of 8 if necessary). The possible remainders for a, b, and c are $0, 1, \ldots, 7$, and squaring and taking remainders yields only the values 0, 1, and 4. To check the possible remainders for $a^2 + b^2 + c^2$ we only need to add together three such terms. (If we get a sum larger than 7 we subtract 8.) A careful analysis of all of the cases shows that we cannot obtain 7 as a remainder for $a^2 + b^2 + c^2$. Thus we cannot express any integer n whose remainder is 7 when divided by 8 in the form $n = a^2 + b^2 + c^2$. □

Trial and error techniques similar to those of Example 1.3.1 can sometimes be used to show that a polynomial equation has no integer solution. For example, if $x = c$ is a solution of the equation $a_k x^k + \ldots + a_1 x + a_0 = 0$, then $a_k c^k + \ldots + a_1 c + a_0$ must be divisible by every integer n. If some n can be found for which $a_k x^k + \ldots + a_1 x + a_0$ is never divisible by n, then this can be used to prove that the equation has no integer solutions. For example, $x^3 + x + 1 = 0$ has no integer solutions since $c^3 + c + 1$ is odd for all integers c, and thus is never divisible by 2.

A more familiar situation in which we carry out arithmetic after dividing by a fixed integer is the addition of hours on a clock (where the fixed integer is 12). Another example is given by the familiar rules "even plus even is even," "even times even is even," etc., which are useful in other circumstances (where the fixed integer is 2). Gauss introduced the following congruence notation, which simplifies computations of this sort.

1.3.1 Definition. *Let n be a positive integer. Integers a and b are said to be* ***congruent modulo*** *n if they have the same remainder when divided by n. This is denoted by writing $a \equiv b \pmod{n}$.*

If we use the division algorithm to write $a = nq + r$, where $0 \leq r < n$, then $r = n \cdot 0 + r$. It follows immediately from the previous definition that $a \equiv r \pmod{n}$. In particular, any integer is congruent modulo n to one of the integers $0, 1, 2, \ldots, n-1$.

We feel that the definition we have given provides the best intuitive understanding of the notion of congruence, but in almost all proofs it will be easiest to use the characterization given by the next proposition. Using this characterization makes it possible to utilize the facts about divisibility that we have developed in the preceding sections of this chapter.

1.3.2 Proposition. *Let a, b, and $n > 0$ be integers. Then $a \equiv b \pmod{n}$ if and only if $n \mid (a - b)$.*

Proof. If $a \equiv b \pmod{n}$, then a and b have the same remainder when divided by n, so the division algorithm gives $a = nq_1 + r$ and $b = nq_2 + r$. Solving for the common remainder gives $a - nq_1 = b - nq_2$. Thus $a - b = n(q_1 - q_2)$, and so $n \mid (a - b)$.

To prove the converse, assume that $n \mid (a - b)$. Then there exists $k \in \mathbf{Z}$ with $a - b = nk$, and hence $b = a - nk$. If upon applying the division algorithm we have $a = nq + r$, with $0 \leq r < n$, then $b = a - nk = (nq + r) - nk = n(q - k) + r$. Since $0 \leq r < n$, division of b by n also yields the remainder r. Hence $a \equiv b \pmod{n}$. □

When working with congruence modulo n, the integer n is called the **modulus**. By the preceding proposition, $a \equiv b \pmod{n}$ if and only if $a - b = nq$ for some integer q. We can write this in the form $a = b + nq$, for some integer q. This observation gives a very useful method of replacing a congruence with an equation (over $\mathbf{Z}$). On the other hand, Proposition 1.3.3 shows that any equation can be converted to a congruence modulo n by simply changing the $=$ sign to $\equiv$. In doing so, any term congruent to 0 can simply be omitted. Thus the equation $a = b + nq$ would be converted back to $a \equiv b \pmod{n}$.

Congruence behaves in many ways like equality. The following properties, which are obvious from the definition of congruence modulo n, are a case in point. Let a, b, c be integers. Then

(i) $a \equiv a \pmod{n}$;

(ii) if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$;

(iii) if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

The following theorem carries this analogy even further. Perhaps its most important consequence is that when adding, subtracting, or multiplying congruences you may substitute any congruent integer. For example, to show that $99^2 \equiv 1 \pmod{100}$, it is easier to substitute -1 for 99 and just show that $(-1)^2 = 1$.

1.3.3 Proposition. *Let $n > 0$ be an integer. Then the following conditions hold for all integers a, b, c, d:*

(a) *If $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then $a \pm b \equiv c \pm d \pmod{n}$, and $ab \equiv cd \pmod{n}$.*

(b) *If $a + c \equiv a + d \pmod{n}$, then $c \equiv d \pmod{n}$. If $ac \equiv ad \pmod{n}$ and $(a, n) = 1$, then $c \equiv d \pmod{n}$.*

Proof. (a) If $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then $n \mid (a - c)$ and $n \mid (b - d)$. Adding shows that $n \mid ((a + b) - (c + d))$, and subtracting shows that $n \mid ((a - b) - (c - d))$. Thus $a \pm b \equiv c \pm d \pmod{n}$.

Since $n \mid (a - c)$, we have $n \mid (ab - cb)$, and then since $n \mid (b - d)$, we must have $n \mid (cb - cd)$. Adding shows that $n \mid (ab - cd)$ and thus $ab \equiv cd \pmod{n}$.

(b) If $a + c \equiv a + d \pmod{n}$, then $n \mid ((a + c) - (a + d))$. Thus $n \mid (c - d)$ and so $c \equiv d \pmod{n}$.

If $ac \equiv ad \pmod{n}$, then $n \mid (ac - ad)$, and since $(n, a) = 1$, it follows from Proposition 1.2.3 (b) that $n \mid (c - d)$. Thus $c \equiv d \pmod{n}$. □

The consequences of Proposition 1.3.3 can be summarized as follows.

(i) For any number in the congruence, you can substitute any congruent integer.

(ii) You can add or subtract the same integer on both sides of a congruence.

(iii) You can multiply both sides of a congruence by the same integer.

(iv) Canceling, or dividing both sides of a congruence by the same integer, must be done very carefully. You may divide both sides of a congruence by an integer a only if $(a, n) = 1$. For example, $30 \equiv 6 \pmod{8}$, but dividing both sides by 6 gives $5 \equiv 1 \pmod{8}$, which is certainly false. On the other hand, since 3 is relatively prime to 8, we may divide both sides by 3 to get $10 \equiv 2 \pmod{8}$.

Proposition 1.3.3 shows that the remainder upon division by n of $a + b$ or ab can be found by adding or multiplying the remainders of a and b when divided by n and then dividing by n again if necessary. For example, if $n = 8$, then 101 has remainder 5 and 142 has remainder 6 when divided by 8. Thus $101 \cdot 142 = 14,342$ has the same remainder as 30 (namely, 6) when divided by 8. Formally, $101 \equiv 5 \pmod{8}$ and $142 \equiv 6 \pmod{8}$, so it follows that $101 \cdot 142 \equiv 5 \cdot 6 \equiv 6 \pmod{8}$.

As a further example, we compute the powers of 2 modulo 7. Rather than computing each power and then dividing by 7, we reduce modulo 7 at each stage of the computations:

$$\begin{aligned} 2^2 &\equiv 4 \pmod{7}, \\ 2^3 &\equiv 2^2 2 \equiv 4 \cdot 2 \equiv 1 \pmod{7}, \\ 2^4 &\equiv 2^3 2 \equiv 1 \cdot 2 \equiv 2 \pmod{7}, \end{aligned}$$

$$2^5 \equiv 2^4 2 \equiv 2 \cdot 2 \equiv 4 \pmod 7.$$

From the way in which we have done the computations, it is clear that the powers will repeat. In fact, since there are only finitely many remainders modulo n, the powers of any integer will eventually begin repeating modulo n.

1.3.4 Proposition. *Let a and $n > 1$ be integers. There exists an integer b such that $ab \equiv 1$ (mod n) if and only if $(a, n) = 1$.*

Proof. If there exists an integer b such that $ab \equiv 1 \pmod n$, then we have $ab = 1 + qn$ for some integer q. This can be rewritten to give a linear combination of a and n equal to 1, and so $(a, n) = 1$.

Conversely, if $(a, n) = 1$, then there exist integers s, t such that $sa + tn = 1$. Letting $b = s$ and reducing the equation to a congruence modulo n gives $ab \equiv 1 \pmod n$. □

We are now ready to present a systematic study of linear congruences that involve unknowns. The previous proposition shows that the congruence

$$ax \equiv 1 \pmod n$$

has a solution if and only if $(a, n) = 1$. In fact, the proof of the proposition shows that the solution can be obtained by using the Euclidean algorithm to write $1 = ab + nq$ for some $b, q \in \mathbf{Z}$, since then $1 \equiv ab \pmod n$.

The next theorem determines all solutions of a linear congruence of the form

$$ax \equiv b \pmod n\ .$$

Of course, if the numbers involved are small, it may be simplest just to use trial and error. For example, to solve $3x \equiv 2 \pmod 5$, we only need to substitute $x = 0, 1, 2, 3, 4$. Thus by trial and error we can find the solution $x \equiv 4 \pmod 5$.

In many ways, solving congruences is like solving equations. There are a few important differences, however. A linear equation over the integers (an equation of the form $ax = b$, where $a \neq 0$) has at most one solution. On the other hand, the linear congruence $2x \equiv 2 \pmod 4$ has the two solutions $x \equiv 1 \pmod 4$ and $x \equiv 3 \pmod 4$.

For linear equations, it may happen that there is no solution. The same is true for linear congruences. For example, trial and error shows that the congruence $3x \equiv 2 \pmod 6$ has no solution. Thus the first step in solving a linear congruence is to use Theorem 1.3.5 to determine whether or not a solution exists.

We say that two solutions r and s to the congruence $ax \equiv b \pmod n$ are **distinct solutions modulo** n if r and s are not congruent modulo n. Thus in the next theorem the statement "d distinct solutions modulo n" means that there are d solutions $s_1, s_2, \ldots, s_d$ such that if $i \neq j$, then s_i and s_j are not congruent modulo n. This terminology is necessary in order to understand what we mean by "solving" the congruence $ax \equiv b \pmod n$. In the next section, we will introduce the concept of a "congruence class" to clarify the situation.

1.3.5 Theorem. *Let a, b and $n > 1$ be integers. The congruence $ax \equiv b$ (mod n) has a solution if and only if b is divisible by d, where $d = (a, n)$. If $d \,|\, b$, then there are d distinct solutions modulo n, and these solutions are congruent modulo n/d.*

Proof. To prove the first statement, observe that $ax \equiv b$ (mod n) has a solution if and only if there exist integers s and q such that $as = b + nq$, or, equivalently, $as + (-q)n = b$. Thus there is a solution if and only if b can be expressed as a linear combination of a and n. By Theorem 1.1.6 the linear combinations of a and n are precisely the multiples of d, so there is a solution if and only if $d \,|\, b$.

To prove the second statement, assume that $d \,|\, b$, and let $m = n/d$. Suppose that x_1 and x_2 are solutions of the congruence $ax \equiv b$ (mod n), giving $ax_1 \equiv ax_2$ (mod n). Then $n \,|\, a(x_1 - x_2)$, and so it follows from Proposition 1.2.3 (a) that $n \,|\, d(x_1 - x_2)$. Thus $m \,|\, (x_1 - x_2)$, and so $x_1 \equiv x_2$ (mod m). On the other hand, if $x_1 \equiv x_2$ (mod m), then $m \,|\, (x_1 - x_2)$, and so $n \,|\, d(x_1 - x_2)$ since $n = dm$. Then since $d \,|\, a$ we can conclude that $n \,|\, a(x_1 - x_2)$, and so $ax_1 \equiv ax_2$ (mod n).

We can choose the distinct solutions from among the remainders $0, 1, \ldots, n-1$. Given one such solution, we can find all others in the set by adding multiples of n/d, giving a total of d distinct solutions. □

We now describe an algorithm for solving linear congruences of the form

$$ax \equiv b \ (\text{mod } n)\ .$$

We first compute $d = (a, n)$, and if $d \,|\, b$, then we write the congruence $ax \equiv b$ (mod n) as an equation $ax = b + qn$. Since d is a common divisor of a, b, and n, we can write $a = da_1$, $b = db_1$, and $n = dm$. Thus we get $a_1 x = b_1 + qm$, which yields the congruence

$$a_1 x \equiv b_1 \ (\text{mod } m)\ ,$$

where $a_1 = a/d$, $b_1 = b/d$, and $m = n/d$.

It follows immediately from Proposition 1.2.10 that since $d = (a, n)$, the numbers a_1 and m must be relatively prime. Thus by Proposition 1.3.4 we can apply the Euclidean algorithm to find an integer c such that $ca_1 \equiv 1$ (mod m). Multiplying both sides of the congruence $a_1 x \equiv b_1$ (mod m) by c gives the solution

$$x \equiv cb_1 \ (\text{mod } m)\ .$$

Finally, since the original congruence was given modulo n, we should give our answer modulo n instead of modulo m. The congruence $x \equiv cb_1$ (mod m) can be converted to the equation $x = cb_1 + mk$, which yields the solution $x \equiv cb_1 + mk$ (mod n). The solution modulo m determines d distinct solutions modulo n. The solutions have the form $s_0 + km$, where s_0 is any particular solution of $x \equiv b_1 c$ (mod m) and k is any integer.

Example 1.3.2 (Homogeneous linear congruences).

In this example we consider the special case of a linear homogeneous congruence

$$ax \equiv 0 \pmod{n} .$$

In this case there always exists a solution, namely $x \equiv 0 \pmod{n}$; but this may not be the only solution modulo n.

As the first step in the solution we obtain $a_1 x \equiv 0 \pmod{n_1}$, where $a = da_1$ and $n = dn_1$. Since a_1 and n_1 are relatively prime, by part (b) of Proposition 1.3.3 we can cancel a_1, to obtain

$$x \equiv 0 \pmod{n_1} , \qquad \text{with } n_1 = \frac{n}{\gcd(a,n)} .$$

We have d distinct solutions modulo n.

For example, $28x \equiv 0 \pmod{48}$ reduces to $x \equiv 0 \pmod{12}$, and $x \equiv 0$, 12, 24, 36 are the four distinct solutions modulo 48. □

Example 1.3.3.

To solve the congruence

$$60x \equiv 90 \pmod{105} ,$$

we first note that $(60, 105) = 15$, and then check that $15 \mid 90$, so that there will indeed be a solution. Dividing the corresponding equation $60x = 90 + 105q$ by 15, we obtain the equation $4x = 6 + 7q$, which reduces to the congruence

$$4x \equiv 6 \pmod{7} .$$

To solve this congruence, we need an integer c with $c \cdot 4 \equiv 1 \pmod{7}$, so in effect we must solve another congruence, $4z \equiv 1 \pmod{7}$. We could use the Euclidean algorithm, but with such a small modulus, trial and error is quicker, and it is easy to see that $c = 2$ will work.

We now multiply both sides of the congruence $4x \equiv 6 \pmod{7}$ by 2, to obtain $8x \equiv 12 \pmod{7}$, which reduces to

$$x \equiv 5 \pmod{7} .$$

Writing the solution in the form of an equation, we have $x = 5 + 7k$, so $x \equiv 5 + 7k \pmod{105}$. By adding multiples of 7 to the particular solution $x_0 = 5$, we obtain the solutions $\ldots, -2, 5, 12, 19, \ldots$. There are 15 distinct solutions modulo 105, so we have

$$x \equiv 5, 12, 19, 26, 33, 40, 47, 54, 61, 68, 75, 82, 89, 96, 103 \pmod{105} . \quad \square$$

In the next theorem we show how to solve two simultaneous congruences over moduli that are relatively prime. The motivation for the proof of the next theorem is as follows. Assume that the congruences $x \equiv a \pmod{n}$ and $x \equiv b \pmod{m}$ are given. If we can find integers y and z with

$$y \equiv 1 \pmod{n} \qquad y \equiv 0 \pmod{m}$$

$$z \equiv 0 \pmod{n} \qquad z \equiv 1 \pmod{m}$$

then $x = ay + bz$ will be a solution to the pair of simultaneous congruences $x \equiv a \pmod{n}$ and $x \equiv b \pmod{m}$. This can be seen by reducing x modulo n and then modulo m.

1.3.6 Theorem (Chinese Remainder Theorem). *Let n and m be positive integers, with $(n, m) = 1$. Then the system of congruences*

$$x \equiv a \pmod{n} \qquad x \equiv b \pmod{m}$$

has a solution. Moreover, any two solutions are congruent modulo mn.

Proof. Since $(n, m) = 1$, there exist integers r and s such that $rm + sn = 1$. Then $rm \equiv 1 \pmod{n}$ and $sn \equiv 1 \pmod{m}$. Following the suggestion in the preceding paragraph, we let $x = arm + bsn$. Then a direct computation verifies that $x \equiv arm \equiv a \pmod{n}$ and $x \equiv bsn \equiv b \pmod{m}$.

If x is a solution, then adding any multiple of mn is obviously still a solution. Conversely, if x_1 and x_2 are two solutions of the given system of congruences, then they must be congruent modulo n and modulo m. Thus $x_1 - x_2$ is divisible by both n and m, so it is divisible by mn since by assumption $(n, m) = 1$. Therefore $x_1 \equiv x_2 \pmod{mn}$. □

Example 1.3.4.

The proof of Theorem 1.3.6 actually shows how to solve the given system of congruences. For example, if we wish to solve the system

$$x \equiv 7 \pmod{8} \qquad x \equiv 3 \pmod{5}$$

we first use the Euclidean algorithm to write $2 \cdot 8 - 3 \cdot 5 = 1$. Then $x = 7(-3)(5) + 3(2)(8) = -57$ is a solution, and the general solution is $x = -57 + 40t$. The smallest nonnegative solution is therefore 23, so we have

$$x \equiv 23 \pmod{40}\ . \ \square$$

Another proof of the existence of a solution in Theorem 1.3.6 can be given as follows. In some respects this method of solution is more intuitive and provides a convenient algorithm for solving the congruences. Given the congruences

$$x \equiv a \pmod{n} \qquad x \equiv b \pmod{m}$$

we can rewrite the first congruence as an equation in the form $x = a + qn$ for some $q \in \mathbf{Z}$. To find a simultaneous solution, we only need to substitute this expression for x in the second congruence, giving $a + qn \equiv b \pmod{m}$, or

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

Since $(n, m) = 1$, we can solve the congruence $nz \equiv 1 \pmod{m}$, and using this solution we can solve for q in the congruence $qn \equiv b - a \pmod{m}$.

Recall that we converted the first congruence $x \equiv a \pmod{m}$ to the equation $x = a + qn$. Now that we have a value for q, we can substitute, and so this gives the simultaneous solutions to the two congruences in the form $x = a + qn$. We can choose as a particular solution the smallest positive integer in this form. The general solution is obtained by adding multiples of mn.

Example 1.3.5.

To illustrate the second method of solution, again consider the system

$$x \equiv 7 \pmod{8} \qquad x \equiv 3 \pmod{5} .$$

The first congruence gives us the equation $x = 7 + 8q$, and then substituting we obtain $7 + 8q \equiv 3 \pmod{5}$, or equivalently, $3q \equiv -4 \pmod{5}$. Multiplying by 2, since $2 \cdot 3 \equiv 1 \pmod{5}$, gives $q \equiv -8 \pmod{5}$ or $q \equiv 2 \pmod{5}$. This yields the particular solution $x = 7 + 2 \cdot 8 = 23$. □

Example 1.3.6 (Difference of squares)**.**

We will use techniques from this section to prove that if m and n are odd integers, then $m^2 - n^2$ is divisible by 8. (Compare Example 1.1.7.)

Proof: We need to show that if m and n are odd, then $m^2 - n^2 \equiv 0 \pmod{8}$. Modulo 8, any odd integer is congruent to either ± 1 or ± 3, and squaring any of these four values gives $1 \pmod{8}$. Thus $m^2 - n^2 \equiv 1 - 1 \equiv 0 \pmod{8}$. □

Example 1.3.7.

For which positive integers n does $a^2 \equiv 0 \pmod{n}$ imply $a \equiv 0 \pmod{n}$?

Answer: We will show that $a^2 \equiv 0 \pmod{n}$ implies $a \equiv 0 \pmod{n}$ if and only if n is not divisible by the square of a prime number.

given as
ovides a

or some
ression

ng this

uation
s gives
n. We
ı. The

First, suppose that n is not divisible by the square of a prime number. Then by the fundamental theorem of arithmetic we can write $n = p_1 p_2 \cdots p_k$ for distinct primes $p_1, p_2, \ldots, p_k$. Then $a^2 \equiv 0 \pmod{n}$ implies $n \mid a^2$, and so for each i we have $p_i \mid a^2$, and hence $p_i \mid a$, for each i. Therefore $p_1 p_2 \cdots p_k \mid a$, and so $a \equiv 0 \pmod{n}$.

To prove the converse, we give a proof by contradiction. If $p^2 \mid n$ for some prime number p, then $n = p^2 t$ for some $t \in \mathbf{Z}$. Letting $a = pt$, it follows that $a^2 \equiv 0 \pmod{n}$ but $a \not\equiv 0 \pmod{n}$. □

EXERCISES: SECTION 1.3

1. Solve the following congruences.

   †(a) $4x \equiv 1 \pmod{7}$

   (b) $2x \equiv 1 \pmod{9}$

   †(c) $5x \equiv 1 \pmod{32}$

   (d) $19x \equiv 1 \pmod{36}$

2. Write n as a sum of four squares for $1 \leq n \leq 20$.

3. Solve the following congruences.

   †(a) $10x \equiv 5 \pmod{21}$

   (b) $10x \equiv 5 \pmod{15}$

   †(c) $10x \equiv 4 \pmod{15}$

   (d) $10x \equiv 4 \pmod{14}$

4. Solve the following congruence. $20x \equiv 12 \pmod{72}$

5.†Solve the following congruence. $25x \equiv 45 \pmod{60}$

6. Find all integers x such that $3x + 7$ is divisible by 11.
   Comment: This was Exercise 25 of Section 1.1; new techniques are available.

7. The smallest positive solution of the congruence $ax \equiv 0 \pmod{n}$ is called the **additive order** of a modulo n. Find the additive orders of each of the following elements, by solving the appropriate congruences.

   †(a) 8 modulo 12

   (b) 7 modulo 12

   †(c) 21 modulo 28

   (d) 12 modulo 18

8. Prove that if p is a prime number and a is any integer such that $p \not| a$, then the additive order of a modulo p is equal to p.

9. Prove that if $n > 1$ and $a > 0$ are integers and $d = (a, n)$, then the additive order of a modulo n is n/d.

10. Let a, b, n be positive integers. Prove that if $a \equiv b \pmod{n}$, then $(a, n) = (b, n)$.

11. Show that 7 is a divisor of $(6! + 1)$, 11 is a divisor of $(10! + 1)$, and 19 is a divisor of $(18! + 1)$.

12. Show that $4 \cdot (n^2 + 1)$ is never divisible by 11.

13. Prove that the sum of the cubes of any three consecutive positive integers is divisible by 9. (Compare Exercise 24 of Section 1.1.)

14. Find the units digit of $3^{29} + 11^{12} + 15$.
Hint: Choose an appropriate modulus n, and then reduce modulo n.

15. Solve the following congruences by trial and error.
†(a) $x^2 \equiv 1 \pmod{16}$
(b) $x^3 \equiv 1 \pmod{16}$
†(c) $x^4 \equiv 1 \pmod{16}$
(d) $x^8 \equiv 1 \pmod{16}$

16. Solve the following congruences by trial and error.
(a) $x^3 + 2x + 2 \equiv 0 \pmod{5}$
(b) $x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod{2}$
(c) $x^4 + x^3 + 2x^2 + 2x \equiv 0 \pmod{3}$

17. List and solve all quadratic congruences modulo 3. That is, list and solve all congruences of the form $ax^2 + bx + c \equiv 0 \pmod{3}$. The only coefficients you need to consider are $0, 1, 2$.

18. Solve the following system of congruences.

$$x \equiv 15 \pmod{27} \qquad x \equiv 16 \pmod{20}$$

19.†Solve the following system of congruences.

$$x \equiv 11 \pmod{16} \qquad x \equiv 18 \pmod{25}$$

20. Solve the following system of congruences.

$$2x \equiv 5 \pmod{7} \qquad 3x \equiv 4 \pmod{8}$$

Hint: First reduce to the usual form.

21. Solve the following system of congruences.

$$x \equiv a \pmod{n} \qquad x \equiv b \pmod{n+1}$$

22. Extend the techniques of the Chinese remainder theorem to solve the following system of congruences.

$$2x \equiv 3 \pmod{7} \qquad x \equiv 4 \pmod{6} \qquad 5x \equiv 50 \pmod{55}$$

23. This exercise extends the Chinese remainder theorem. Let m, n be positive integers, with $(m, n) = d$ and $[m, n] = k$. Prove that the system of congruences

$$x \equiv a \pmod{n} \qquad x \equiv b \pmod{m}$$

has a solution if and only if $a \equiv b \pmod{d}$, and in this case any two solutions are congruent modulo k.

24. (Casting out nines) Show that the remainder of an integer n when divided by 9 is the same as the remainder of the sum of its digits when divided by 9.
Hint: For example, $7862 \equiv 7 + 8 + 6 + 2 \pmod{9}$. How you can use the digits of 7862 to express it in terms of powers of 10?
Note: "Casting out nines" is a traditional method for checking a sum of a long column of large numbers by reducing each of the numbers modulo 9 and checking the sum modulo 9. This exercise shows that the method is practical, because it provides a quick algorithm for reducing an integer modulo 9.

25. Find a result similar to casting out nines for the integer 11.

26.‡Prove that the fourth power of an integer can only have 0, 1, 5, or 6 as its units digit.

27. Let p be a prime number and let a, b be any integers. Prove that

$$(a + b)^p \equiv a^p + b^p \pmod{p} .$$

28. Prove that in any Pythagorean triple (a, b, c), either a or b is divisible by 3, and one of a, b, c is divisible by 5.

29. Prove that there exist infinitely many prime numbers of the form $4m + 3$ (where m is an integer).

30.‡An integer of the form $F_n = 2^{2^n} + 1$, for $n \in \mathbf{Z}$, $n \geq 0$, is called a **Fermat number**.

(a) Show that if $m \in \mathbf{Z}$, $m \geq 0$, such that $2^m + 1$ is prime, then $m = 0$ or m is a power of 2.

(b) Show that F_5 is divisible by 641, providing a counterexample to Fermat's belief that all Fermat numbers are prime.

(c) Show that $F_n \equiv 7 \pmod{10}$ for $n \geq 2$.

(d) Show that $\prod_{0 \leq n < m} F_n = F_m - 2$.

(e) Show that $(F_n, F_m) = 1$ if $n \neq m$.

(f) Use part (e) to give a new proof that there are infinitely many prime numbers.