Congruences

Divisibility is a powerful tool in the theory of numbers. We have seen this amply demonstrated in work on Pythagorean triples, greatest common divisors, and factorization into primes. In this chapter we will discuss the theory of congruences. Congruences provide a convenient way to describe divisibility properties. In fact, they are so convenient and natural that they make the theory of divisibility very similar to the theory of equations.

We say that a *is congruent to* b *modulo* m, and we write

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

if m divides $a - b$. For example,

$$7 \equiv 2 \pmod{5} \qquad \text{and} \qquad 47 \equiv 35 \pmod{6},$$

since

$$5|(7-2) \qquad \text{and} \qquad 6|(47-35).$$

In particular, if a divided by m leaves a remainder of r, then a is congruent to r modulo m. Notice that the remainder satisfies $0 \le r < m$, so every integer is congruent, modulo m, to a number between 0 and $m-1$.

The number m is called the *modulus* of the congruence. Congruences with the same modulus behave in many ways like ordinary equations. Thus, if

$$\begin{aligned} a_1 \equiv b_1 \pmod{m} \quad \text{and} \quad a_2 \equiv b_2 \pmod{m}, \quad \text{then} \\ a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m} \quad \text{and} \quad a_1 a_2 \equiv b_1 b_2 \pmod{m}. \end{aligned}$$

Warning. It is not always possible to divide congruences. In other words, if $ac \equiv bc \pmod{m}$, it need not be true that $a \equiv b \pmod{m}$. For example,

$15 \cdot 2 \equiv 20 \cdot 2 \pmod{10}$, but $15 \not\equiv 20 \pmod{10}$. Even more distressing, it is possible to have

$$uv \equiv 0 \pmod{m} \text{ with } u \not\equiv 0 \pmod{m} \text{ and } v \not\equiv 0 \pmod{m}.$$

Thus $6 \cdot 4 \equiv 0 \pmod{12}$, but $6 \not\equiv 0 \pmod{12}$ and $4 \not\equiv 0 \pmod{12}$. However, if $\gcd(c, m) = 1$, then it is okay to cancel c from the congruence $ac \equiv bc \pmod{m}$. You will be asked to verify this as an exercise.

Congruences with unknowns can be solved in the same way that equations are solved. For example, to solve the congruence

$$x + 12 \equiv 5 \pmod{8},$$

we subtract 12 from each side to get

$$x \equiv 5 - 12 \equiv -7 \pmod{8}.$$

This solution is fine, or we can use the equivalent solution $x \equiv 1 \pmod{8}$. Notice that -7 and 1 are the same modulo 8, since their difference is divisible by 8.

Here's another example. To solve

$$4x \equiv 3 \pmod{19},$$

we will multiply both sides by 5. This gives

$$20x \equiv 15 \pmod{19}.$$

But $20 \equiv 1 \pmod{19}$, so $20x \equiv x \pmod{19}$. Thus the solution is

$$x \equiv 15 \pmod{19}.$$

We can check our answer by substituting 15 into the original congruence. Is $4 \cdot 15 \equiv 3 \pmod{19}$? Yes, because $4 \cdot 15 - 3 = 57 = 3 \cdot 19$ is divisible by 19.

We solved this last congruence by a trick, but if all else fails, there's always the "climb every mountain" technique.[1] To solve a congruence modulo m, we can just try each value $0, 1, \ldots, m-1$ for each variable. For example, to solve the congruence

$$x^2 + 2x - 1 \equiv 0 \pmod{7},$$

we just try $x = 0$, $x = 1$, …, $x = 6$. This leads to the two solutions $x \equiv 2 \pmod{7}$ and $x \equiv 3 \pmod{7}$. Of course, there are other solutions, such as $x \equiv 9 \pmod{7}$.

[1] Also known as the "ford every stream" technique for those who prefer wet feet to vertigo.

But 9 and 2 are not really different solutions, since they are the same modulo 7. So when we speak of "finding all the solutions to a congruence," we normally mean that we will find all incongruent solutions, that is, all solutions that are not congruent to one another.

We also observe that there are many congruences, such as $x^2 \equiv 3 \pmod{10}$, that have no solutions. This shouldn't be too surprising. After all, there are ordinary equations such as $x^2 = -1$ that have no (real) solutions.

Our final task in this chapter is to solve congruences that look like

$$ax \equiv c \pmod{m}.$$

Some congruences of this type have no solutions. For example, if

$$6x \equiv 15 \pmod{514}$$

were to have a solution, then 514 would have to divide $6x - 15$. But $6x - 15$ is always odd, so it cannot be divisible by the even number 514. Hence the congruence $6x \equiv 15 \pmod{514}$ has no solutions.

Before giving the general theory, let's try an example. We will solve the congruence

$$18x \equiv 8 \pmod{22}.$$

This means we need to find a value of x with 22 dividing $18x - 8$, so we have to find a value of x with $18x - 8 = 22y$ for some y. In other words, we need to solve the linear equation

$$18x - 22y = 8.$$

We know that we can solve the equation

$$18u - 22v = \gcd(18, 22) = 2,$$

and indeed we easily find the solution $u = 5$ and $v = 4$. But we really want the right-hand side to equal 8, so we multiply by 4 to get

$$18 \cdot (5 \cdot 4) - 22 \cdot (4 \cdot 4) = 8.$$

Thus, $18 \cdot 20 \equiv 8 \pmod{22}$, so $x \equiv 20 \pmod{22}$ is a solution to the original congruence. We will soon see that this congruence has two different solutions modulo 22; the other one turns out to be $x \equiv 9 \pmod{22}$.

Suppose now that we are asked to solve an arbitrary congruence of the form

$$ax \equiv c \pmod{m}.$$

We need to find an integer x such that m divides $ax - c$. The number m will divide the number $ax - c$ if we can find an integer y such that $ax - c = my$. Rearranging this last equation slightly, we see that $ax \equiv c \pmod{m}$ has a solution if, and only if, the linear equation $ax - my = c$ has a solution.

To make our formulas a bit neater, we will let $g = \gcd(a, m)$. Our first observation is that every number of the form $ax - my$ is a multiple of g; so if g does not divide c, then $ax - my = c$ has no solutions and so $ax \equiv c \pmod{m}$ also has no solutions.

Next suppose that g does divide c. We know from the Linear Equation Theorem that there is always a solution to the equation

$$au + mv = g.$$

Suppose we find a solution $u = u_0$, $v = v_0$, either by trial and error or by using the Euclidean algorithm method. Since we are assuming that g divides c, we can multiply this equation by the integer c/g to obtain the equation

$$a\frac{cu_0}{g} + m\frac{cv_0}{g} = c.$$

This means that

$$x_0 \equiv \frac{cu_0}{g} \pmod{m} \quad \text{is a solution to the congruence} \quad ax \equiv c \pmod{m}.$$

Are there other solutions? Suppose that x_1 is some other solution to the congruence $ax \equiv c \pmod{m}$. Then $ax_1 \equiv ax_0 \pmod{m}$, so m divides $ax_1 - ax_0$. This implies that

$$\frac{m}{g} \quad \text{divides} \quad \frac{a(x_1 - x_0)}{g},$$

and we know that m/g and a/g have no common factors, so m/g must divide $x_1 - x_0$. In other words, there is some number k such that

$$x_1 = x_0 + k \cdot \frac{m}{g}.$$

But any two solutions that differ by a multiple of m are considered to be the same, so there will be exactly g different solutions that are obtained by taking $k = 0, 1, \ldots, g - 1$.

This completes our analysis of the congruence $ax \equiv c \pmod{m}$. We summarize our findings in the following statement.

Theorem 1 (Linear Congruence Theorem)**.** *Let a, c, and m be integers with $m \geq 1$, and let $g = \gcd(a, m)$.*

(a) *If $g \nmid c$, then the congruence $ax \equiv c \pmod{m}$ has no solutions.*

(b) *If $g|c$, then the congruence $ax \equiv c \pmod{m}$ has exactly g incongruent solutions. To find the solutions, first find a solution (u_0, v_0) to the linear equation*

$$au + mv = g.$$

Then $x_0 = cu_0/g$ is a solution to $ax \equiv c \pmod{m}$, and a complete set of incongruent solutions is given by

$$x \equiv x_0 + k \cdot \frac{m}{g} \pmod{m} \quad \textit{for } k = 0, 1, 2, \ldots, g-1.$$

For example, the congruence

$$943x \equiv 381 \pmod{2576}$$

has no solutions, since $\gcd(943, 2576) = 23$ does not divide 381. On the other hand, the congruence

$$893x \equiv 266 \pmod{2432}$$

has 19 solutions, since $\gcd(893, 2432) = 19$ does divide 266. Notice that we are able to determine the number of solutions without having computed any of them. To actually find the solutions, we first solve

$$893u - 2432v = 19.$$

We find the solution $(u, v) = (79, 29)$. Multiplying by $266/19 = 14$ gives the solution

$$(x, y) = (1106, 406) \qquad \text{to the equation} \qquad 893x - 2432y = 266.$$

Finally, the complete set of solutions to

$$893x \equiv 266 \pmod{2432}$$

is obtained by starting with $x \equiv 1106 \pmod{2432}$ and adding multiples of the quantity $2432/19 = 128$. (Don't forget that if the numbers go above 2432 we are allowed to subtract 2432.) The 19 incongruent solutions are

$$1106, 1234, 1362, 1490, 1618, 1746, 1874, 2002, 2130, 2258,$$
$$2386, 82, 210, 338, 466, 594, 722, 850, 978.$$

Important Note. The most important case of the Linear Congruence Theorem is when $\gcd(a, m) = 1$. In this case, it says that the congruence

$$ax \equiv c \pmod{m} \qquad (*)$$

has exactly one solution. We might even write the solution as a fraction

$$x \equiv \frac{c}{a} \pmod{m},$$

but if we do, then we must remember that the symbol "$\frac{c}{a} \pmod{m}$" is really only a convenient shorthand for the solution to the congruence $(*)$.

Nonlinear congruences are also very important in number theory. As an example, consider the congruence

$$x^2 + 1 \equiv 0 \pmod{m}$$

whose solutions are square roots of -1 modulo m. For some values of m such as $m = 5$ and $m = 13$, there are solutions,

$$2^2 + 1 \equiv 0 \pmod{5} \qquad \text{and} \qquad 5^2 + 1 \equiv 0 \pmod{13},$$

while for other values such as $m = 3$ and $m = 7$, there are no solutions.

You probably already know that a polynomial of degree d with real coefficients has no more than d real roots.[2] This well-known "fact" is not true for congruences, since for example the congruence

$$x^2 + x \equiv 0 \pmod{6}$$

has four distinct roots modulo 6, namely 0, 2, 3, and 5. However, if we look at congruences modulo primes, then order and harmony are restored to the world. And although the statement of the following theorem may seem innocuous, we will see later that it is a powerful tool for proving many important results.

Theorem 2 (Polynomial Roots Mod p Theorem)**.** *Let p be a prime number and let*

$$f(x) = a_0x^d + a_1x^{d-1} + \cdots + a_d$$

be a polynomial of degree $d \geq 1$ with integer coefficients and with $p \nmid a_0$. Then the congruence

$$f(x) \equiv 0 \pmod{p}$$

has at most d incongruent solutions.

[2] In fact, the Fundamental Theorem of Algebra implies that a polynomial of degree d with complex coefficients always has exactly d complex roots, provided that you count multiple roots appropriately.

There are many ways to prove this important theorem, but for the sake of variety and to introduce you to a new mathematical tool, we give a "Proof by Contradiction."[3] In a proof by contradiction, we begin by making a statement. We then use that statement to make deductions, eventually ending up with a conclusion that is clearly false. This allows us to deduce that the original statement was false, since it led to a false conclusion.

The particular statement with which we begin is the following:

$$\textbf{Statement}: \begin{cases} \text{There exists at least one polynomial } F(x) \text{ with integer} \\ \text{coefficients and with leading coefficient not divisible by} \\ p \text{ such that the congruence } F(x) \equiv 0 \pmod{p} \text{ has more} \\ \text{distinct roots modulo } p \text{ than its degree.} \end{cases}$$

Now among all such polynomials, we choose one having smallest possible degree, say

$$F(x) = A_0x^d + A_1x^{d-1} + A_2x^{d-2} + \cdots + A_d.$$

Then we let

$$r_1, r_2, \ldots, r_{d+1}$$

be distinct mod p solution to the congruence

$$F(x) \equiv 0 \pmod{p}.$$

We are going to use the fact that for any value of r, the difference $F(x) - F(r)$ can be factored. To see this, we write

$$F(x) - F(r) = A_0(x^d - r^d) + A_1(x^{d-1} - r^{d-1}) + \cdots + A_{d-1}(x - r).$$

Each term $x^i - r^i$ has a factor of $x - r$, since

$$x^i - r^i = (x - r)(x^{i-1} + x^{i-2}r + x^{i-3}r^2 + \cdots + xr^{i-2} + r^{i-1}).$$

Pulling an $x - r$ out of each term, we find that

$$F(x) - F(r) = (x - r)(\text{some messy polynomial of degree } d - 1).$$

In other words, there is a polynomial

$$G(x) = B_0x^{d-1} + B_1x^{d-2} + \cdots + B_{d-2}x + B_{d-1}$$

[3]The classical Latin phrase for "proof by contradiction" is *reductio ad absurdum*, literally "reduction to an absurdity." As G.H. Hardy says in his monograph *A Mathematician's Apology*, proof by contradiction "is one of a mathematician's finest weapons. It is a far finer gambit than any chess gambit: a chess player may offer the sacrifice of a pawn or even a piece, but a mathematician offers *the game*."

of degree $d-1$ such that

$$F(x) = F(r) + (x-r)G(x).$$

In particular, if we substitute $r = r_1$ and use the fact that $F(r_1) \equiv 0 \pmod{p}$, we find that

$$F(x) \equiv (x-r_1)G(x) \pmod{p}.$$

We have assumed that $F(x) \equiv 0 \pmod{p}$ has $d+1$ distinct incongruent solutions $x = r_1, r_2, \ldots, r_{d+1}$. If we substitute one of the solutions r_k with $k \geq 2$ for x, we find that

$$0 \equiv F(r_k) \equiv (r_k - r_1)G(r_k) \pmod{p}.$$

We know that $r_1 \not\equiv r_k \pmod{p}$, so the Prime Divisibility Property tells us that $G(r_k) \equiv 0 \pmod{p}$. (Note that this is where we use the assumption that the modulus p is prime. Do you see why the argument would fall apart if the modulus were composite?)

We now know that $r_2, r_3, \ldots, r_{d+1}$ are solutions to $G(x) \equiv 0 \pmod{p}$. Thus $G(x)$ is a polynomial of degree $d-1$ that has d distinct roots modulo p. This contradicts the fact that among such polynomials, the polynomial $F(x)$ was one having the smallest possible degree. Hence the original statement must be false, which shows that there are no polynomials having more roots modulo p than their degree. Stated in a positive manner, we have proven that every polynomial of degree d has at most d roots modulo p. This completes the proof of Theorem 2.

Exercises

1. Suppose that $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$.
(a) Verify that $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$ and that $a_1 - a_2 \equiv b_1 - b_2 \pmod{m}$.
(b) Verify that $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

2. Suppose that

$$ac \equiv bc \pmod{m}$$

and also assume that $\gcd(c, m) = 1$. Prove that $a \equiv b \pmod{m}$.

3. Find all incongruent solutions to each of the following congruences.
(a) $7x \equiv 3 \pmod{15}$ **(b)** $6x \equiv 5 \pmod{15}$
(c) $x^2 \equiv 1 \pmod{8}$ **(d)** $x^2 \equiv 2 \pmod{7}$
(e) $x^2 \equiv 3 \pmod{7}$

4. Prove that the following divisibility tests work.
(a) The number a is divisible by 4 if and only if its last two digits are divisible by 4.

(b) The number a is divisible by 8 if and only if its last three digits are divisible by 8.
(c) The number a is divisible by 3 if and only if the sum of its digits is divisible by 3.
(d) The number a is divisible by 9 if and only if the sum of its digits is divisible by 9.
(e) The number a is divisible by 11 if and only if the alternating sum of the digits of a is divisible by 11. (If the digits of a are $a_1a_2a_3\dots a_{d-1}a_d$, the alternating sum means to take $a_1 - a_2 + a_3 - \cdots$ with alternating plus and minus signs.)

[*Hint*. For (a), reduce modulo 100, and similarly for (b). For (c), (d), and (e), write a as a sum of multiples of powers of 10 and reduce modulo 3, 9, and 11.]

5. Find all incongruent solutions to each of the following linear congruences.
(a) $8x \equiv 6 \pmod{14}$
(b) $66x \equiv 100 \pmod{121}$
(c) $21x \equiv 14 \pmod{91}$

6. Determine the number of incongruent solutions for each of the following congruences. You need not write down the actual solutions.
(a) $72x \equiv 47 \pmod{200}$
(b) $4183x \equiv 5781 \pmod{15087}$
(c) $1537x \equiv 2863 \pmod{6731}$

7. 💻 Write a program that solves the congruence

$$ax \equiv c \pmod{m}.$$

[If $\gcd(a, m)$ does not divide c, return an error message and the value of $\gcd(a, m)$.] Test your program by finding all of the solutions to the congruences in Exercise 6.

8. 💻 Write a program that takes as input a positive integer m and a polynomial $f(X)$ having integer coefficients and produces as output all of the solutions to the congruence

$$f(X) \equiv 0 \pmod{m}.$$

(Don't try to be fancy. Just substitute $X = 0, 1, 2, \dots m - 1$ and see which values are solutions.) Test your program by taking the polynomial

$$f(X) = X^{11} + 21X^7 - 8X^3 + 8$$

and solving the congruence $f(X) \equiv 0 \pmod{m}$ for each of the following values of m,

$$m \in \{130,\ 137,\ 144,\ 151,\ 158,\ 165,\ 172\}.$$

9. (a) How many solutions are there to the congruence

$$X^4 + 5X^3 + 4X^2 - 6X - 4 \equiv 0 \pmod{11} \quad \text{with } 0 \le X < 11?$$

Are there four solutions, or are there fewer than four solutions?

(b) Consider the congruence $X^2 - 1 \equiv 0 \pmod 8$. How many solutions does it have with $0 \leq X < 8$? Notice that there are more than two solutions. Why doesn't this contradict the Polynomial Roots Mod p Theorem (Theorem 2)?

10. Let p and q be distinct primes. What is the maximum number of possible solutions to a congruence of the form

$$x^2 - a \equiv 0 \pmod{pq},$$

where as usual we are only interested in solutions that are distinct modulo pq?