

1.3 Congruences

In this section, it is important to remember that although working with congruences is almost like working with equations, it is not exactly the same.

What things are the same? You can add or subtract the same integer on both sides of a congruence, and you can multiply both sides of a congruence by the same integer. You can use substitution, and you can use the fact that if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$. (Review Proposition 1.3.3, and the comments in the text both before and after the proof of the proposition.)

What things are different? In an ordinary equation you can divide through by a nonzero number. In a congruence modulo n , you can only divide through by an integer that is relatively prime to n . This is usually expressed by saying that if $\gcd(a, n) = 1$ and $ac \equiv ad \pmod{n}$, then $c \equiv d \pmod{n}$. Just be very careful!

One of the important techniques to understand is how to switch between congruences and ordinary equations. First, any equation involving integers can be converted into a congruence by just reducing modulo n . This works because if two integers are equal, then are certainly congruent modulo n .

The do the opposite conversion you must be more careful. If two integers are congruent modulo n , that doesn't make them equal, but only guarantees that dividing by n produces the same remainder in each case. In other words, the integers may differ by some multiple of n .

The conversion process is illustrated in Example 1.3.5 of the text, where the congruence

$$x \equiv 7 \pmod{8}$$

is converted into the equation

$$x = 7 + 8q, \text{ for some } q \in \mathbf{Z}.$$

Notice that converting to an equation makes it more complicated, because we have to introduce another variable. In the example, we really want a congruence modulo 5, so the next step is to rewrite the equation as

$$x \equiv 7 + 8q \pmod{5}.$$

Actually, we can reduce each term modulo 5, so that we finally get

$$x \equiv 2 + 3q \pmod{5}.$$

You should read the proofs of Theorem 1.3.5 and Theorem 1.3.6 very carefully. These proofs actually show you the necessary techniques to solve all linear congruences of the form $ax \equiv b \pmod{n}$, and all simultaneous linear equations of the form $x \equiv a \pmod{n}$ and $x \equiv b \pmod{m}$, where the moduli n and m are relatively prime. Many of the theorems in the text should be thought of as "shortcuts", and you can't afford to skip over their proofs, because you might miss important algorithms or computational techniques.

SOLVED PROBLEMS: §1.3

26. Solve the congruence $42x \equiv 12 \pmod{90}$.
27. (a) Find all solutions to the congruence $55x \equiv 35 \pmod{75}$.
(b) Find all solutions to the congruence $55x \equiv 36 \pmod{75}$.
28. (a) Find one particular integer solution to the equation $110x + 75y = 45$.
(b) Show that if $x = m$ and $y = n$ is an integer solution to the equation in part (a), then so is $x = m + 15q$ and $y = n - 22q$, for any integer q .
29. Solve the system of congruences $x \equiv 2 \pmod{9}$ $x \equiv 4 \pmod{10}$.
30. Solve the system of congruences $5x \equiv 14 \pmod{17}$ $3x \equiv 2 \pmod{13}$.
31. Solve the system of congruences $x \equiv 5 \pmod{25}$ $x \equiv 23 \pmod{32}$.
32. Give integers a, b, m, n to provide an example of a system

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

that has no solution.

33. (a) Compute the last digit in the decimal expansion of 4^{100} .
(b) Is 4^{100} divisible by 3?
34. Find all integers n for which $13 \mid 4(n^2 + 1)$.
35. Prove that $10^{n+1} + 4 \cdot 10^n + 4$ is divisible by 9, for all positive integers n .
36. Prove that the fourth power of an integer can only have 0, 1, 5, or 6 as its units digit.