

Congruences

A congruence is a statement about divisibility. It is a notation that simplifies reasoning about divisibility. It suggests proofs by its analogy to equations. Congruences are familiar to us as “clock arithmetic.” Four hours after 10 AM it will be 2 PM. How do we get the 2 from the 10 and the 4? We add four to ten and then subtract 12. We have used a congruence modulo 12.

Definition: Suppose a and b are integers and m is a positive integer. If m divides $a - b$, then we say a **is congruent to b modulo m** and write $a \equiv b \pmod{m}$. If m does not divide $a - b$, we say a **is not congruent to b modulo m** and write $a \not\equiv b \pmod{m}$. The formula $a \equiv b \pmod{m}$ is called a **congruence**. The integer m is called the **modulus** (plural **moduli**) of the congruence.

Do not confuse the binary operator “mod” in $a \bmod b$, which means the remainder when a is divided by b , with the “mod” enclosed in parentheses together with the modulus of a congruence. These concepts are related as follows. If m is a positive integer and a and b are integers, then $a \equiv b \pmod{m}$ if and only if $(a \bmod m) = (b \bmod m)$.

We will often use the fact that $a \equiv b \pmod{m}$ if and only if there is an integer k so that $a = b + km$. This fact follows immediately from the definitions of congruence and divide.

The congruence relation has many similarities to equality. The following theorem says that congruence, like equality, is an equivalence relation.

THEOREM: Let m be a positive integer. Let a , b and c be integers. Then:

1. $a \equiv a \pmod{m}$.
2. If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.
3. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Let $m > 0$ be fixed. For each integer a , the set of all integers $b \equiv a \pmod{m}$ is called the **congruence class** or **residue class** of a modulo m . The congruence class of a modulo m consists of all integers in the arithmetic progression $a + dm$, where d runs through all integers. Each integer in a congruence class is a **representative** of it. If the modulus m is understood and a and b are in the same congruence class, then each is called a **residue** of the other. The smallest nonnegative representative of a congruence class is often used as the standard representative of it. For example, the standard representative of the congruence class of $27 \pmod{5}$ is 2.

THEOREM: Let a , b , c and d be integers. Let m be a positive integer. Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then

1. $a + c \equiv b + d \pmod{m}$.

2. $a - c \equiv b - d \pmod{m}$.

3. $ac \equiv bd \pmod{m}$.

Let a and b be integers. Let m be a positive integer. Let f be a polynomial with integer coefficients. If $a \equiv b \pmod{m}$, then $f(a) \equiv f(b) \pmod{m}$.

Let a and b be integers. Let m and d be positive integers with $d|m$. If $a \equiv b \pmod{m}$, then $a \equiv b \pmod{d}$.

Although the arithmetic operations of addition, subtraction and multiplication for congruences obey the usual rules for the same operations with integers, division does not always work as for integers. For example, $2 \cdot 3 = 6 \equiv 18 = 2 \cdot 9 \pmod{12}$, but $3 \not\equiv 9 \pmod{12}$.

In general $ac \equiv bc \pmod{m}$ does not always imply $a \equiv b \pmod{m}$. We now investigate when this implication will be true.

THEOREM: If $\gcd(a, m) = 1$, then there is a unique x in $0 < x < m$ such that $ax \equiv 1 \pmod{m}$.

Proof: The function $f(i) = (ai \pmod{m})$ for $1 \leq i \leq m - 1$ is one-to-one, and so the set

$$\{ai \pmod{m}; i = 1, \dots, m - 1\}$$

is a permutation of $\{1, \dots, m - 1\}$. Therefore 1 appears exactly once in the first set, that is, there is exactly one x in $0 < x < m$ such that $ax \equiv 1 \pmod{m}$.

Note that the x in this theorem is like “ a^{-1} ,” the reciprocal of a modulo m . Sometimes we even use the notation “ $a^{-1} \pmod{m}$ ” to mean the x of this theorem.

THEOREM: If $m > 1$, a, b, c are integers, ($c \neq 0$), $\gcd(c, m) = 1$, then $ac \equiv bc \pmod{m}$ implies $a \equiv b \pmod{m}$.

Proof: By the previous theorem, there is an x such that $cx \equiv 1 \pmod{m}$. Then $ac \equiv bc \pmod{m}$ implies $acx \equiv bcx \pmod{m}$, which implies $a1 \equiv b1 \pmod{m}$, which implies $a \equiv b \pmod{m}$.

Definition: A set of m integers r_1, \dots, r_m is a **complete set of residues (CSR) modulo m** if every integer is congruent modulo m to exactly one of the r_i 's.

The set $\{1, \dots, m\}$ is called the standard CSR modulo m .

Linear Congruences

We now tell how to solve congruences like $ax \equiv b \pmod{m}$, where a , b and $m > 1$ are given integers and x is an unknown integer. The solution to an equation $ax = b$, where $a \neq 0$, is the single number $x = a/b$. In contrast, if the congruence $ax \equiv b \pmod{m}$ has any solution, then infinitely many integers x satisfy it.

For example, the solution to the congruence $2x \equiv 1 \pmod{5}$ is all integers of the form $x = 5k + 3$, where k may be any integer, that is, x lies in the arithmetic progression

$$\dots, -12, -7, -2, 3, 8, 13, 18, \dots$$

This set of integers may be described compactly as $x \equiv 3 \pmod{5}$. We could have written this solution as $x \equiv 28 \pmod{5}$, but we generally use the least nonnegative residue as the standard representative of its congruence class.

THEOREM: Let $m > 1$, a and b be integers. Then $ax \equiv b \pmod{m}$ has a solution if and only if $\gcd(a, m)$ divides b .

THEOREM: Let $m > 1$, a and b be integers. Let $g = \gcd(a, m)$. If $g|b$, then $ax \equiv b \pmod{m}$ has g solutions. They are

$$x \equiv \frac{b}{g}x_0 + t\frac{m}{g} \pmod{m}, \quad t = 0, 1, \dots, g - 1,$$

where x_0 is any solution of $\frac{a}{g}x_0 \equiv 1 \pmod{\frac{m}{g}}$. This means that

$$x = \frac{b}{g}x_0 + t\frac{m}{g}, \quad t = 0, 1, \dots,$$

are all integer solutions x .

Example: Solve $7x \equiv 3 \pmod{12}$.

We find $g = \gcd(7, 12) = 1$ and $g|b$ since $1|3$, so there is one solution. Since $7 \cdot 7 \equiv 1 \pmod{12}$, we have $x_0 = 7$, and the solution to $7x \equiv 3 \pmod{12}$ is $x = 3 \cdot 7 + t \cdot 12 = 21 + 12t \equiv 9 \pmod{12}$.

Example: Solve $165x \equiv 100 \pmod{285}$.

In an earlier example, we calculated that $\gcd(165, 285) = 15$. Since 15 does not divide 100, the congruence has no solution.

Example: Solve $165x \equiv 105 \pmod{285}$.

As above, we have $\gcd(165, 285) = 15$. Since $15|105$, the congruence has fifteen solutions modulo 285. To find them, we first solve the congruence $(165/15)x_0 \equiv 1 \pmod{(285/15)}$, or $11x_0 \equiv 1 \pmod{19}$. The extended Euclidean algorithm gives $11(7) + 19(-4) = 1$, so $x_0 = 7$. Then $x = (105/15)(7) + t(19) = 7 \cdot 7 + 19t$. The fifteen solutions are

$$x = 7, 7 + 19, 7 + 2 \cdot 19, \dots, 7 + 14 \cdot 19,$$

that is, $x \equiv 7, 26, 45, 64, \dots$, or $273 \pmod{285}$. These solutions are the same numbers as $x \equiv 7 \pmod{19}$.