CONGRUENCE EQUATIONS

A *polynomial congruence equation* or, simply, a *congruence equation* (in one unknown x) is an equation of the form

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 \pmod{m} \qquad (1)$$

Such an equation is said to be of *degree* n if $a \not\equiv 0 \pmod{m}$.

Suppose $s \equiv t \pmod{m}$. Then s is a solution of (1) if and only if t is a solution of (1). Thus the *number of solutions* of (1) is defined to be the number of incongruent solutions or, equivalently, the number of solutions in the set

$$\{0, 1, 2, \ldots, m-1\}$$

Of course, these solutions can always be found by testing, that is, by substituting each of the m numbers into (1) to see if it does indeed satisfy the equation.

EXAMPLE Consider the equations:

(a) $x^2 + x + 1 \equiv 0 \pmod{4}$, (b) $x^2 + 3 \equiv 0 \pmod{6}$, (c) $x^2 - 1 \equiv 0 \pmod{8}$

Here we find the solutions by testing.

(a) There are no solutions since 0, 1, 2, and 3 do not satisfy the equation.

(b) There is only one solution among $0, 1, \ldots, 5$ which is 3. Thus the general solution consists of the integers $3 + 6k$ where $k \in \mathbf{Z}$.

(c) There are four solutions, 1, 3, 5, and 7. This shows that a congruence equation of degree n can have more than n solutions.

Remark : The coefficients of a congruence equation can always be reduced modulo m since an *equivalent* equation, that is, an equation with the same solutions, would result. For example, the following are equivalent equations since the coefficients are congruent modulo $m = 6$:

$$15x^2 + 28x + 14 \equiv 0 \pmod{6}, \quad 3x^2 + 4x + 2 \equiv 0 \pmod{6}, \quad 3x^2 - 2x + 2 \equiv 0 \pmod{6},$$

Usually we choose coefficients between 0 and $m - 1$

Linear Congruence Equation: $ax \equiv 1 \pmod{m}$

First we consider the special linear congruence equation

$$ax \equiv 1 \pmod{m} \qquad (11.\ )$$

where $a \not\equiv 0 \pmod{m}$. The complete story of this equation is given in the following theorem

Theorem .: If a and m are relatively prime, then $ax \equiv 1 \pmod{m}$ has a unique solution; otherwise it has no solution.

EXAMPLE

(a) Consider the congruence equation $6x \equiv 1 \pmod{33}$. Since $\gcd(6, 33) = 3$, this equation has no solution.

(b) Consider the congruence equation $7x \equiv 1 \pmod{9}$. Since $\gcd(7, 9) = 1$, the equation has a unique solution. Testing the numbers $0, 1, \ldots, 8$, we find that

$$7(4) = 28 \equiv 1 \pmod{9}$$

Thus $x = 4$ is our unique solution. (The general solution is $4 + 9k$ for $k \in \mathbf{Z}$.)

Suppose a solution of (11) does exist, that is, suppose $\gcd(a, m) = 1$. Furthermore, suppose the modulus m is large. Then the Euclidean algorithm can be used to find a solution of (11). Specifically, we use the Euclidean algorithm to find x_0 and y_0 such that

$$ax_0 + my_0 = 1$$

From this it follows that $ax_0 \equiv 1 \pmod{m}$; that is, x_0 is a solution to (11).

EXAMPLE Consider the following congruence equation:

$$81 \equiv 1 \pmod{256}$$

By observation or by applying the Euclidean algorithm to 81 and 256, we find that $\gcd(81, 256) = 1$. Thus the equation has a unique solution. Testing may not be an efficient way to find this solution since the modulus $m = 256$ is relatively large. Hence, we apply the Euclidean algorithm to $a = 81$ and $m = 256$. Specifically, as in Example , we find $x_0 = -25$ and $y_0 = 7$ such that

$$81x_0 + 256y_0 = 1$$

This means that $x_0 = -25$ is a solution of the given congruence equation. Adding $m = 256$ to -25, we obtain the following unique solution between 0 and 256:

$$x = 231$$

Linear Congruence Equation: $ax \equiv b \pmod{m}$

Now we consider the more general linear congruence equation

$$ax \equiv b \pmod{m} \qquad (11.1)$$

where $a \not\equiv 0 \pmod{m}$. We first consider the case where a and m are coprime.

Theorem : Suppose a and m are relatively prime. Then $ax \equiv b \pmod{m}$ has a unique solution. Moreover, if s is the unique solution to $ax \equiv 1 \pmod{m}$, then the unique solution to $ax \equiv b \pmod{m}$ is $x = bs$.

EXAMPLE

(a) Consider the congruence equation $3x \equiv 5 \pmod 8$. Since 3 and 8 are coprime, the equation has a unique solution. Testing the integers $0, 1, \ldots, 7$, we find that

$$3(7) = 21 \equiv 5 \pmod 8$$

Thus $x = 7$ is the unique solution of the equation.

(b) Consider the linear congruence equation

$$33x \equiv 38 \pmod{280}$$

Since $\gcd(33, 280) = 1$, the equation has a unique solution. Testing may not be an efficient way to find this solution since the modulus $m = 280$ is relatively large. We apply the Euclidean algorithm to first find a solution to

$$33x \equiv 1 \pmod{280}$$

That is, as in Example , we find $x_0 = 17$ and $y_0 = 2$ to be a solution of

$$33x_0 + 280y_0 = 1$$

This means that $s = 17$. Then

$$sb = 17(38) = 646$$

is a solution . Dividing 646 by $m = 280$, we obtain the remainder

$$x = 86$$

which is the unique solution between 0 and 280. (The general solution is $86 + 280k$ with $k \in \mathbf{Z}$.)

Theorem : Consider the equation $ax \equiv b \pmod m$ where $d = \gcd(a, m)$.

(i) Suppose d does not divide b. Then $ax \equiv b \pmod m$ has no solution.

(ii) Suppose d does divide b. Then $ax \equiv b \pmod m$ has d solutions which are all congruent modulo M to the unique solution of

$$Ax \equiv B \pmod M \quad \text{where} \quad A = a/d,\ B = b/d,\ M = m/d.$$

We emphasize that Theorem 11.27 applies to the equation $Ax \equiv B \pmod M$ in Theorem since $\gcd(A, M) = 1$.

EXAMPLE Solve each congruence equation: (a) $4x \equiv 9 \pmod{14}$; (b) $8x \equiv 12 \pmod{28}$.

(a) Note $\gcd(4, 14) = 2$. However, 2 does not divide 9. Hence the equation does not have a solution.

(b) Note that $d = \gcd(8, 28) = 4$, and $d = 4$ does divide 12. Thus the equation has $d = 4$ solutions. Dividing each term in the equation by $d = 4$ we obtain the congruence equation (11.7) which has a unique solution.

$$2x \equiv 3 \pmod 7$$

Testing the integers $0, 1, \ldots, 6$, we find that 5 is the unique solution of (11.7). We now add $d - 1 = 3$ multiples of 7 to the solution 5 obtaining:

$$5 + 7 = 12, \quad 5 + 2(7) = 19, \quad 5 + 3(7) = 26$$

Accordingly, 5, 12, 19, 26 are the required $d = 4$ solutions of the original equation $8x \equiv 12 \pmod{28}$.