3.3: Linear Congruences

Because congruences are analogous to equations, it is natural to ask about solutions of linear equations. In this section, we will be discussing linear congruences of one variable and their solutions. We start by defining linear congruences.

A congruence of the form \(ax \equiv b \pmod{m}\) where \(x\) is an unknown integer is called a linear congruence in one variable.

It is important to know that if \(x_0\) is a solution for a linear congruence, then all integers \(x_i\) such that \(x_i \equiv x_0 \pmod{m}\) are solutions of the linear congruence. Notice also that \(ax \equiv b \pmod{m}\) is equivalent to a linear Diophantine equation i.e. there exists \(y\) such that \(ax-my=b\). We now prove theorems about the solutions of linear congruences.

Let \(a, b\) and \(m\) be integers such that \(m>0\) and let \(c=(a,m)\). If \(c\) does not divide \(b\), then the congruence \(ax \equiv b \pmod{m}\) has no solutions. If \(c\mid b\), then \([ax\equiv b\pmod{m}]\) has exactly \(c\) incongruent solutions modulo \(m\).

As we mentioned earlier, \([ax\equiv b\pmod{m}]\) is equivalent to \([ax-my=b]\). By Theorem 19 on Diophantine equations, we know that if \(\gcd(c)\) does not divide \(b\), then the equation, \([ax-my=b]\) has no solutions. Notice also that if \(\gcd(c)\mid b\), then there are infinitely many solutions whose variable \(x\) is given by \([x=x_0+(m/c)t]\) Thus the above values of \(x\) are solutions of the congruence \([ax\equiv b\pmod{m}]\). Now we have to determine the number of incongruent solutions that we have. Suppose that two solutions are congruent, i.e. \([x_0+(m/c)t_1\equiv x_0+(m/c)t_2\pmod{m}]\) Thus we get \([t_1\equiv t_2\pmod{c}]\) and thus \([t_1\equiv t_2\pmod{c}]\) Thus we get a set of incongruent solutions given by \([x=x_0+(m/c)t]\), where \(t\) is taken modulo \(c\).

Notice that if \(\gcd(c)=(a,m)=1\), then there is a unique solution modulo \(m\) for the equation \([ax\equiv b\pmod{m}]\).
Let us find all the solutions of the congruence \((3x \equiv 12 \mod 6)\). Notice that \((3, 6) = 3\) and \(3 \mid 12\). Thus there are three incongruent solutions modulo \(6\). We use the Euclidean algorithm to find the solution of the equation \((3x - 6y = 12)\) as described in chapter 2. As a result, we get \((x, 0 = 6)\). Thus the three incongruent solutions are given by \((x_1 = 6 \mod 6)\), \((x_1 = 6 + 2 = 2 \mod 6)\) and \((x_2 = 6 + 4 = 4 \mod 6)\).

As we mentioned earlier in Remark 2, the congruence \((ax \equiv b \mod m)\) has a unique solution if \((a, m) = 1\). This will allow us to talk about modular inverses.

A solution for the congruence \((ax \equiv 1 \mod m)\) for \((a, m) = 1\) is called the modular inverse of \(a\) modulo \(m\). We denote such a solution by \(\bar{a}\).

The modular inverse of 7 modulo 48 is 7. Notice that a solution for \((7x \equiv 1 \mod 48)\) is \((x \equiv 7 \mod 48)\).

**Exercises**

1. Find all solutions of \((3x \equiv 6 \mod 9)\).
2. Find all solutions of \((3x \equiv 2 \mod 7)\).
3. Find an inverse modulo 13 of 2 and of 11.
4. Show that if \(\bar{a}\) is the inverse of \(a\) modulo \(m\) and \(\bar{b}\) is the inverse of \(b\) modulo \(m\), then \((\bar{a}\bar{b})\) is the inverse of \((ab)\) modulo \(m\).

**Contributors**

- Dr. Wissam Raji, Ph.D., of the American University in Beirut. His work was selected by the Saylor Foundation’s Open Textbook Challenge for public release under a Creative Commons Attribution (CC BY) license.