3.1: Introduction to Congruences

As we mentioned in the introduction, the theory of congruences was developed by Gauss at the beginning of the nineteenth century.

Let \( m \) be a positive integer. We say that \( a \) is congruent to \( b \) modulo \( m \) if \( m \mid (a-b) \) where \( a \) and \( b \) are integers, i.e. if \( a=b+km \) where \( k \in \mathbb{Z} \).

If \( a \equiv b \pmod{m} \), we write \( a \equiv b \pmod{m} \).

\( 19 \equiv 5 \pmod{7} \). Similarly \( 2k+1 \equiv 1 \pmod{2} \) which means every odd number is congruent to 1 modulo 2.

There are many common properties between equations and congruences. Some properties are listed in the following theorem.

**Theorem: Properties of Congruences**

Let \( a, b, c \) and \( d \) denote integers. Let \( m \) be a positive integer. Then:

1. If \( a \equiv b \pmod{m} \), then \( b \equiv a \pmod{m} \).
2. If \( a \equiv b \pmod{m} \) and \( b \equiv c \pmod{m} \), then \( a \equiv c \pmod{m} \).
3. If \( a \equiv b \pmod{m} \), then \( a+c \equiv b+c \pmod{m} \).
4. If \( a \equiv b \pmod{m} \), then \( a-c \equiv b-c \pmod{m} \).
5. If \( a \equiv b \pmod{m} \), then \( ac \equiv bc \pmod{m} \), for \( c \neq 0 \).
6. If \( a \equiv b \pmod{m} \), then \( ac \equiv bc \pmod{m} \), for \( c \neq 0 \).
7. If \( a \equiv b \pmod{m} \) and \( c \equiv d \pmod{m} \), then \( a+c \equiv b+d \pmod{m} \).
8. If \( a \equiv b \pmod{m} \) and \( c \equiv d \pmod{m} \), then \( a-c \equiv b-d \pmod{m} \).
1. If \(a \equiv b (mod \ m)\), then \(m \mid (a-b)\). Thus there exists integer \(k\) such that \((a-b)=mk\), this implies \((b-a)=m(-k)\) and thus \(m \mid (b-a)\). Consequently \((b \equiv a (mod \ m))\).

2. Since \(a \equiv b (mod \ m)\), then \(m \mid (a-b)\). Also, \(c \equiv d (mod \ m)\), then \(m \mid (c-d)\). As a result, there exist two integers \(k\) and \(l\) such that \((a=b+mk)\) and \((b=c+ml)\), which imply that \((a=c+m(k+l))\) giving that \((a\equiv c (mod \ m))\).

3. Since \(a \equiv b (mod \ m)\), then \(m \mid (a-b)\). So if we add and subtract \(c\) we get \(m \mid ((a+c)-(b+c))\) and as a result \([a+c] \equiv [b+c] (mod \ m).]\)

4. Since \(a \equiv b (mod \ m)\), then \(m \mid (a-b)\) so we can subtract and add \(c\) and we get \(m \mid ((a-c)-(b-c))\) and as a result \([a-c] \equiv [b-c] (mod \ m).]\)

5. If \(a \equiv b (mod \ m)\), then \(m \mid (a-b)\). Thus there exists integer \(k\) such that \((a-b)=mk\) and as a result \((ac-bc)=m(kc)\). Thus \(m \mid (ac-bc)\) and hence \([ac] \equiv [bc] (mod \ m).]\)

6. If \(a \equiv b (mod \ m)\), then \(m \mid (a-b)\). Thus there exists integer \(k\) such that \((a-b)=mk\) and as a result \((ac-bc)=m(kc)\). Thus \(mc \mid (ac-bc)\) and hence \([ac] \equiv [bc] (mod \ mc).]\)

7. Since \(a \equiv b (mod \ m)\), then \(m \mid (a-b)\). Also, \(c \equiv d (mod \ m)\), then \(m \mid (c-d)\). As a result, there exist two integers \(k\) and \(l\) such that \((a-b)=mk\) and \((c-d)=ml\). Note that \(((a-b)+(c-d))=(a+c)-(b+d)=m(k+l)\). As a result, \([a+c] \equiv [b+d] (mod \ m).]\)

8. There exist two integers \(k\) and \(l\) such that \((a-b)=mk\) and \((c-d)=ml\) and thus \([ca-cb] \equiv [bc-bd] (mod \ m).]\) Note that \((ca-cb)+(bc-bd)=ac-bd=m(kc-lb).\) As a result, \([m \mid (ac-bd),]\) hence \([ac] \equiv [bc] (mod \ m).]\)

9. Because \(14 \equiv 8 (mod \ 6)\) then \(8 \equiv 14 (mod \ 6).\)

10. Because \(22 \equiv 10 (mod \ 6)\) and \(10 \equiv 4 (mod \ 6).\) Notice that \(22 \equiv 4 (mod \ 6).\)

11. Because \(50 \equiv 20 (mod \ 15).\) Then \(50+5=55 \equiv 20+5=25 (mod \ 15).\)

12. Because \(50 \equiv 20 (mod \ 15).\) Then \(50-5=45 \equiv 20-5=15 (mod \ 15).\)

13. Because \(19 \equiv 16 (mod \ 3).\) Then \(2(19)=38 \equiv 2(16)=32 (mod \ 3).\)

14. Because \(19 \equiv 16 (mod \ 3).\) Then \(2(19)=38 \equiv 2(16)=32 (mod \ 2(3)=6).\)

15. Because \(19 \equiv 3 (mod \ 8).\) \(17 \equiv 9 (mod \ 8).\) Then \(19+17=36 \equiv 9+12 (mod \ 8).\)

16. Because \(19 \equiv 3 (mod \ 8).\) \(17 \equiv 9 (mod \ 8).\) Then \(19-17=2 \equiv 3-9=-6 (mod \ 8).\)

17. Because \(19 \equiv 3 (mod \ 8).\) \(17 \equiv 9 (mod \ 8).\) Then \(19(17)=323 \equiv 9(27)=27 (mod \ 8).\)

We now present a theorem that will show one difference between equations and congruences. In equations, if we divide both sides of the equation by a non-zero number, equality holds. While in congruences, it is not necessarily true. In other words, dividing both sides of the congruence by the same integer doesn’t preserve the congruence.

1. If \((a,b,c)\) and \((m)\) are integers such that \((m \mid (d=(m,c))\) and \((ac \equiv bc (mod \ m))\), then \((a \equiv b (mod \ m/d))\).

2. If \((m,c=1)\) then \((a=b (mod \ m))\) if \((ac \equiv bc (mod \ m))\).

Part 2 follows immediately from Part 1. For Part 1, if \((ac \equiv bc (mod \ m))\), then \((m \mid (ac-bc))=(a-b)\). Hence there exists \((k)\) such that \((c(a-b)=mk)\). Dividing both sides by \((d)\), we get \([(c/d)(a-b)=k(m/d)].\) Since \(((m/d,c/d)=1))\), it follows that \((m/d \mid (a-b))\). Hence \((a \equiv b (mod \ m/d))\).
\((38 \equiv 10 \pmod{7})\). Since \((2,7)=1\) then \((19 \equiv 5 \pmod{7})\)

The following theorem combines several congruences of two numbers with different moduli.

If \(\{a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_t}\}\) where \((a,b,m_1,m_2,\ldots,m_t)\) are integers and \((m_1,m_2,\ldots,m_t)\) are positive, then \(\langle a \equiv b \pmod{\langle m_1,m_2,\ldots,m_t\rangle}\rangle]\)

Since \((a \equiv b \pmod{m_i})\) for all \(1 \leq i \leq t\). Thus \((m_i \mid (a-b))\). As a result, \(\langle m_1,m_2,\ldots,m_t\rangle \mid (a-b)\) (prove this as an exercise). Thus \(\{a \equiv b \pmod{\langle m_1,m_2,\ldots,m_t\rangle}\}\)

**Exercises**

1. Determine whether 3 and 99 are congruent modulo 7 or not.
2. Show that if \(x\) is an odd integer, then \(x^2 \equiv 1 \pmod{8}\)
3. Show that if \((a,b, m)\) and \((n)\) are integers such that \((m)\) and \((n)\) are positive, \((n \mid m)\) and \(\{a \equiv b \pmod{m}\}\), then \(\{a \equiv b \pmod{n}\}\)
4. Show that if \(\{a_i \equiv b_i \pmod{m}\}\) for \(i=1,2,\ldots,n\), where \((m)\) is a positive integer and \((a_i,b_i)\) are integers for \(i=1,2,\ldots,n\), then \(\sum_{i=1}^n a_i \equiv \sum_{i=1}^n b_i \pmod{m}\)
5. For which \((n)\) does the expression \((1+2+\ldots+(n-1) \equiv 0 \pmod{n})\) holds.

**Contributors and Attributions**

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