

9. Congruences

Definition

Let a, b, m be integers with $m \geq 1$. Then a is congruent to b modulo m if $m \mid (a-b)$. In such a case, we write $a \equiv b \pmod{m}$.

For example,

$$\begin{aligned} 15 &\equiv 4 \pmod{11} && \text{as } 11 \mid (15-4), \\ 23 &\equiv -5 \pmod{14} && \text{as } 14 \mid (23-(-5)) = 28. \end{aligned}$$

Theorem 1

Suppose that a, m are integers with $m \geq 1$. Then there is a *unique* integer r with

- (1) $0 \leq r < m$,
- (2) $a \equiv r \pmod{m}$.

This is just the Division Theorem in disguise. That Theorem states that there are unique integers q, r with $a = qm+r$, and $0 \leq r < m$.

Then $a - r = qm$, so that $m \mid (a-r)$. From the definition, this gives $a \equiv r \pmod{m}$.

Note. Congruence modulo 1 is not very interesting. For *any* integers a, b , we have $1 \mid (a-b)$, so $a \equiv b \pmod{1}$. Thus, *any* two integers are congruent modulo 1.

There are strong similarities between the statements " $a \equiv b \pmod{m}$ " and " $a = b$ ".

Theorem 2 Let a, b, m be integers with $m \geq 1$. Then

- (1) $a \equiv a \pmod{m}$
- (2) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$
- (3) $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$.

Proof

Parts (1) and (2) are easy – we leave these as exercises.

For part (3), suppose that $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$.

Then, from the definition of congruence, $m \mid (a-b)$ and $m \mid (b-c)$.

It follows that $m \mid ((a-b)+(b-c)) = (a-c)$.

Thus, $a \equiv c \pmod{m}$.

The next result shows that the congruence property is related to the arithmetic operations of addition and multiplication.

Theorem 3 Let a, b, c, d, k, m, n are integers, with $m, n \geq 1$. Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then

- (1) $a+c \equiv b+d \pmod{m}$,
- (2) $a+k \equiv b+k \pmod{m}$,
- (3) $ac \equiv bd \pmod{m}$,
- (4) $an \equiv bn \pmod{mn}$ – note the modulus!
- (5) $a^n \equiv b^n \pmod{m}$.

Proof

Since we are given that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, we have integers u, v with $a-b = um$ and $c-d = vm$.

We rearrange these as

$$a = b+um, \text{ and } c = d+vm. \quad (*)$$

For (1), we must look at the difference $(a+c)-(b+d)$ and use (*). We have

$$(a+c)-(b+d) = (b+um)+(d+vm)-b-d = (u+v)m = wm \text{ with } w = (u+v) \in \mathbf{Z}.$$

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

We leave (2) as an exercise to the reader. Hint. Look at $(a+k)-(b+k)$.

For (3), we look at the difference $ac-bd$ and use (*). We get

$$ac-bd = (b+um)(d+vm)-bd = (ud+bv+uvm)m = tm \text{ with } t = (ud+bv+uvm) \in \mathbf{Z}.$$

Thus, $ac \equiv bd \pmod{m}$

For (4), we have $an-bn = (a-b)n = (um)n = u(mn)$, and $u \in \mathbf{Z}$.

Thus $an \equiv bn \pmod{mn}$ as $an-bn$ is a multiple of mn (not just of m)

We do not give a formal proof of (5). We observe that part (3) shows that we can multiply congruences modulo m . Taking powers is just repeated multiplication.

Exercise to the reader

If a, b, k and m are as in the theorem, show that $ak \equiv bk \pmod{m}$.

Note. The similarity between equality and congruence modulo m (for fixed m) is illustrated by parts (1) and (3) of Theorem 3. These say that we can add or multiply the corresponding sides of two (or more) *congruences*, just as we could for equalities.

Earlier, we made use of the fact that $2^{10} = 1024$. It is useful to know the values of the first few powers of 2. By direct calculation, we have

$$2^2 = 4, 2^3 = 8, 2^4 = 16, 2^5 = 32, 2^6 = 64, 2^7 = 128, 2^8 = 256$$

Example Prove that (1) $31 \mid (2^{30} - 1)$, and (2) $65 \mid (2^{66} + 1)$.

Solution

For (1), observe that $2^5 = 32 = 31 + 1$, so $2^5 \equiv 1 \pmod{31}$. Then

$$\begin{aligned} 2^{30} &= (2^5)^6 \\ &\equiv 1^6 \pmod{31} && \text{as } 2^5 \equiv 1 \pmod{31}, \text{ and using Theorem 3(5)} \\ &\equiv 1 \pmod{31} && \text{as } 1^6 = 1 \end{aligned}$$

Thus $2^{30} \equiv 1 \pmod{31}$, so

$$31 \mid (2^{30} - 1), \quad \text{by the definition of congruence}$$

For (2), observe that $2^6 = 64 = 65 + (-1)$, so $2^6 \equiv -1 \pmod{65}$. Then

$$\begin{aligned} 2^{66} &= (2^6)^{11} \\ &\equiv (-1)^{11} \pmod{65} && \text{as } 2^6 \equiv -1 \pmod{65}, \text{ and using Theorem 3(5)} \\ &\equiv -1 \pmod{65} && \text{as } (-1)^{11} = -1 \end{aligned}$$

Thus $2^{66} \equiv -1 \pmod{65}$, so

$$65 \mid (2^{66} + 1), \quad \text{by the definition of congruence}$$

Note. A perfectly good answer would be obtained by omitting the explanations at the right end of various lines

We observe that these solutions relied on selecting powers of 2 *close to* the desired moduli 31 and 65, respectively. Sometimes, some persistence is needed.

Example Show that $41 \mid (2^{20} - 1)$.

Solution

Note that $2^5 = 32 = 41 - 9$, so $2^5 \equiv -9 \pmod{41}$.

$$\text{Then } 2^{10} = (2^5)^2 \equiv (-9)^2 \equiv 81 \equiv -1 \pmod{41}$$

$$\text{Hence, } 2^{20} = (2^{10})^2 \equiv (-1)^2 \equiv 1 \pmod{41}$$

Finally, as $2^{20} \equiv 1 \pmod{41}$, by the definition of congruence, $41 \mid (2^{20} - 1)$.

Example Show that $2^{600} - 1$ is divisible by 63, and by 65.

Solution Observe that 63 and 65 are both close to $2^6 = 64$.

$$2^6 = 64 \equiv 1 \pmod{63}$$

$$\begin{aligned} 2^{600} &= (2^6)^{100} \\ &\equiv 1^{100} \pmod{63} && \text{as } 2^6 \equiv 1 \pmod{63}, \text{ and using Theorem 3(5)} \\ &\equiv 1 \pmod{63} && \text{as } 1^{100} = 1 \end{aligned}$$

Thus $63 \mid (2^{600} - 1)$.

$$2^6 = 64 \equiv -1 \pmod{65}$$

$$\begin{aligned} 2^{600} &= (2^6)^{100} \\ &\equiv (-1)^{100} \pmod{65} && \text{as } 2^6 \equiv -1 \pmod{65}, \text{ and using Theorem 3(5)} \\ &\equiv 1 \pmod{65} && \text{as } (-1)^{100} = 1 \end{aligned}$$

Thus $65 \mid (2^{600} - 1)$.

In this next example, we make use of the fact that the statement $a \mid b$ is equivalent to the statement $b \equiv 0 \pmod{a}$. This follows since the latter, *by its definition*, means that $a \mid (b-0)$, i.e. that $a \mid b$.

Example Show that, for any $n \in \mathbf{N}$, $7 \mid (3^{2n} + 6 \cdot 2^n)$.

Solution

As $3^2 = 9 \equiv 2 \pmod{7}$, $3^{2n} \equiv (3^2)^n \equiv 2^n \pmod{7}$. (Theorem 3(5) again)

Then $3^{2n} + 6 \cdot 2^n \equiv 2^n + 6 \cdot 2^n \equiv (1+6) \cdot 2^n \equiv 7 \cdot 2^n \equiv 0 \cdot 2^n \equiv 0 \pmod{7}$.

In other words, $7 \mid (3^{2n} + 6 \cdot 2^n)$.

Example Suppose we are told that, in the decimal calculation $1234567.9999 = 1234443543?$, where the final digit is illegible, what is that digit?

Solution

Observe that, if a is the final digit in the *decimal* representation of an integer n , then $n \equiv a \pmod{10}$, and, of course $0 \leq a \leq 9$.

Now $1234567 \equiv 7 \pmod{10}$ and $9999 \equiv 9 \pmod{10}$.

Then $1234567.9999 \equiv 7.9 \equiv 63 \equiv 3 \pmod{10}$.

Thus the final digit is a 3.

Look-up tables

For a given positive integer m , we know that any integer n is congruent modulo m to *one* of the integers in the range $0, \dots, m-1$. From Theorem 3, we also know that, in performing arithmetic operations modulo m , each integer may be replaced by the corresponding integer in this range. If we have to perform a large volume of arithmetic, it is more efficient to construct addition and multiplication tables. Then the result of each operation may be read from the table.

For example, working modulo 5, we have

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

x	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

To construct an entry in either table, we add (or multiply) the numbers a , b , and reduce the answer modulo 5, and enter the result in the row labelled a , and the column labelled b .

For example, $3 \times 4 = 12 \equiv 2 \pmod{5}$, $3 + 4 = 7 \equiv 2 \pmod{5}$. This gives us the entries in the last column (label 4) of the penultimate row (label 3).

The tables can be used to expedite calculations modulo 5. Looking up tables is much quicker than doing arithmetic. For example, $4 \times (4+4) \equiv 4 \times 3 \equiv 2 \pmod{5}$.

The rule of 9

There are a number of traditional tests for divisibility by certain integers. Perhaps the best-known is *the rule of 9*.

The decimal number $N = a_{n-1}a_{n-2}\dots a_2a_1$ is divisible by 9

$$\Leftrightarrow a_{n-1} + a_{n-2} + \dots + a_2 + a_1 \text{ is divisible by 9.}$$

Justification

From its decimal form, $N = a_{n-1}10^{n-1} + a_{n-2}10^{n-2} + \dots + a_210 + a_1$

Now, $10 \equiv 1 \pmod{9}$, so, by Theorem 3(5) $10^k \equiv 1^k \equiv 1 \pmod{9}$ for any $k \in \mathbf{N}$.

Hence, by repeated use of Theorem 3, $N \equiv a_{n-1} + a_{n-2} + \dots + a_2 + a_1 \pmod{9}$.

Thus $9 \mid N \Leftrightarrow 9 \mid a_{n-1} + a_{n-2} + \dots + a_2 + a_1$.

Example Which of the integers 1548 and 3451 is divisible by 9?

Solution

$1+5+4+8 = 18$. As $9 \mid 18$, $9 \mid 1548$.

$3+4+5+8 = 20$. As $9 \nmid 20$, $9 \nmid 3451$

Exercise to the reader Show that $3 \mid N \Leftrightarrow 3 \mid a_{n-1} + a_{n-2} + \dots + a_2 + a_1$

Hint. $10 \equiv 1 \pmod{3}$.

There is a similar rule for divisibility by 11, based on the fact $10 \equiv -1 \pmod{11}$.

Rule of 11

$N = a_{n-1}a_{n-2}\dots a_2a_1$ is divisible by 11 $\Leftrightarrow a_{n-1}-a_{n-2}+a_{n-3}-\dots$ is divisible by 11.

Theorem 3 relates congruences to the operations of addition and multiplication. We could have added the result for subtraction, but this is easily derived from our earlier results.

Example Suppose that a, b, c, d, m , are integers with $m \geq 1$.
If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a-c \equiv b-d \pmod{m}$.

Solution

As $c \equiv d \pmod{m}$, $-c \equiv -d \pmod{m}$, by an exercise after Theorem 3.
Then by Theorem 3(1), $a+(-c) \equiv b+(-d) \pmod{m}$ i.e. $a-c \equiv b-d \pmod{m}$.

The case of division is not so simple.

Theorem 4 Let $m, n \in \mathbf{N}$, $a, b \in \mathbf{Z}$. Then

$$Na \equiv Nb \pmod{m} \Leftrightarrow a \equiv b \pmod{M}, \text{ where } M \text{ is the integer } m/\gcd(m, n).$$

Proof

Let $d = \gcd(m, n)$. Then $d \mid m$ and $d \mid n$, so $M = m/d$ and $N = n/d$ are integers.

Also, by Theorem ??, $\gcd(M, N) = 1$. (*)

Now suppose that $na \equiv nb \pmod{m}$. Then, by the definition of congruence,

$$na-nb = n(a-b) = mt, \text{ with } t \in \mathbf{Z}.$$

Dividing through by d , and using $M = m/d$, $N = n/d$, we have

$$N(a-b) = Mt, \text{ with } t \in \mathbf{Z}.$$

Thus $M \mid N(a-b)$.

We also have $\gcd(M, N) = 1$, so Euclid's Lemma gives

$$M \mid (a-b).$$

But this is precisely the condition $a \equiv b \pmod{M}$.

As a special case, we have the

Corollary If $\gcd(m,n) = 1$, then $na \equiv nb \pmod{m} \Leftrightarrow a \equiv b \pmod{m}$

This follows easily from the theorem, since once we have $d = 1$, $M = m/d = m$.

It is useful to remember this as

If $na \equiv nb \pmod{m}$ and $\gcd(m,n) = 1$, then $a \equiv b \pmod{m}$.

In other words, provided $\gcd(m,n) = 1$, we can cancel n from each side of a congruence modulo m .

Examples

(1) $3x \equiv 6 \pmod{8} \Leftrightarrow x \equiv 2 \pmod{8}$, as $\gcd(8,3) = 1$.

(2) $3x \equiv 6 \pmod{9} \Leftrightarrow x \equiv 2 \pmod{3}$, as $\gcd(9,3) = 3$.