Multiples of an Integer Modulo Another Integer

Nitin Verma
mathsanew.com

December 5, 2020

When we repeatedly add an integer a and keep taking *mod* of the results with another integer n (i.e. perform $(a + a + \ldots) \bmod n$), we can find some interesting relations. In this article, we sequentially derive some of these relations.

Let us first get introduced to some very basic concepts of *Modular Arithmetic.*

Some Basics of Modular Arithmetic

We will use $\mathbb{Z}$ to represent the set of all integers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$, and $\mathbb{Z}_n$ to represent the set of integers $\{0, 1, 2, \ldots, n-1\}$. Below is a very fundamental theorem about division of integers.

Theorem 1 (Division Theorem)**.** *For any integers a, n with $n > 0$, there exist unique integers q and r such that $0 \leq r < n$ and $a = qn + r$.*

q and r are called the *Quotient* and *Remainder* of this division respectively. r is always non-negative and will be represented as $a \bmod n$. Note that, for all integers a, $(a \bmod n) \in \mathbb{Z}_n$.

For any a, since $r \geq 0$, we can write: $a \geq qn$. So, if $a < 0$, then $q < 0$. If $q < 0$, then $qn \leq -n$. And since $r < n$, so if $q < 0$, then $a = qn + r < -n + n = 0$.

Thus, in brief, we can write $q < 0$ *iff* $a < 0$.

Note that, for any a, $a \bmod n$ and $(-a) \bmod n$ need not be same. For example, $3 \bmod 10 = 3$, but $(-3) \bmod 10 = 7$.

For any integers a and b, if $a \bmod n = b \bmod n$, we say "a is equivalent to b modulo n", and denote this fact as: $a \equiv b \pmod{n}$. This happens *iff* n divides $(a - b)$. Notice this use of the term "mod n", which is also used as a binary operator like "$a \bmod n$".

The case when $a \bmod n \neq b \bmod n$, is denoted by $a \not\equiv b \pmod{n}$.

It is easy to see that for all integers b such that $b = a + nk$ for some integer k, $a \equiv b \pmod{n}$.

Here are some other useful facts about the mod operation. a, b, n, i are any integers, $n > 0, i \geq 0$. Please convince yourself of the reasoning behind these. Their basis is that any integer a can be expressed as a multiple of n, plus $a \bmod n$ (Division Theorem).

$$
\begin{array}{lrl}
(1) & (a+b) \bmod n &= (a \bmod n + b \bmod n) \bmod n \\
(2) & (a-b) \bmod n &= (a \bmod n - b \bmod n) \bmod n \\
(3) & (ab) \bmod n &= (a(b \bmod n)) \bmod n \\
 & &= ((a \bmod n)b) \bmod n \\
 & &= ((a \bmod n)(b \bmod n)) \bmod n \\
(4) & (a^i) \bmod n &= ((a \bmod n)(a \bmod n) \ldots \{i \text{ times}\}) \bmod n \\
 & &= (a \bmod n)^i \bmod n \\
(5) & a \bmod n &= b \bmod n \\
\Leftrightarrow & (a-b) \bmod n &= (b-a) \bmod n = 0 \\
(6) & (a \pm bn) \bmod n &= a \bmod n
\end{array}
$$

Multiples of a Modulo n

Suppose a, n are any integers with $n > 0$. For $i = 0, 1, 2, \ldots, n-1$, i.e. $i \in \mathbb{Z}_n$, what are the values obtained by $(ai) \bmod n$? Below we will prove a theorem which helps us to find them.

If we know such values for $i \in \mathbb{Z}_n$, we can trivially figure out $(aj) \bmod n$ for any integer j, because $(aj) \bmod n = (a(j \bmod n)) \bmod n$, and $(j \bmod n) \in \mathbb{Z}_n$.

Theorem 2. *For any integers a, n with $n > 0$, $a \bmod n \neq 0$, and $g = gcd(a, n)$, the set of integers $A = \{(ai) \bmod n : i \in \mathbb{Z}_n\}$ is same as set $G = \{0, g, 2g, \ldots, ((n/g) - 1)g\}$.*

Proof. We will represent the value $(ak) \bmod n$, for any integer k (not necessarily in $\mathbb{Z}_n$), as v_k.

For any integer a, say $a' = a \bmod n$, and so $a' \in \mathbb{Z}_n$. Thus, any value $v_i = (ai) \bmod n = ((a \bmod n)i) \bmod n = (a'i) \bmod n$. That means, the set of values obtained for a and a' are exactly the same.

Thus, for the purpose of our proof we can assume $a \in \mathbb{Z}_n$, and the theorem will stand proved for any integer a.

Say, t is the least positive integer such that $v_t = 0$. That is,

$$(at) \bmod n = 0 \quad \Leftrightarrow \quad n \mid at \quad \Leftrightarrow \quad at \text{ is a multiple of } n$$

Since $a \in \mathbb{Z}_n$ and $a \bmod n \neq 0$, so $a > 0$. Also, $t > 0$, implying $at > 0$. Say $m > 0$ is an integer such that $nm = at$. But this is a positive common-multiple of a and n. Since we are looking for the least such t, so:

$$\begin{aligned} & at = lcm(a, n) \\ \Leftrightarrow \quad & at = an/gcd(a, n) = an/g \\ \Leftrightarrow \quad & \;\; t = n/g \end{aligned}$$

Note, g being the gcd of a and n, n/g is an integer. The desired value t is n/g. If $g > 1$, $t = n/g$ is in $\mathbb{Z}_n$.

But if $g = 1$, $t = n$, i.e. t is not in $\mathbb{Z}_n$. That means, $(ai) \bmod n = 0$ is attained only for $i = 0$ in $\mathbb{Z}_n$.

Now, consider all $i < t$, i.e. $i = 0, 1, 2, \ldots, t - 1$. Say, for some i_1 and i_2 among these, with $i_1 < i_2$, we obtain same value of v_i. Then,

$$(ai_1) \bmod n = (ai_2) \bmod n \quad \Leftrightarrow \quad (a(i_2 - i_1)) \bmod n = 0$$

Say $t' = i_2 - i_1$. So, $(at') \bmod n = 0$. But $0 < (i_2 - i_1) < t$. So, $0 < t' < t$, which is impossible since t is the least positive integer with $(at) \bmod n = 0$.

Hence, for all $i < t$ in $\mathbb{Z}_n$, values v_i are distinct. Note that when $g = 1$, in which case $t = n$, all v_i for $i = 0, 1, 2, \ldots, n-1$ are distinct.

Now, for any positive integer j, consider v_{t+j}: $v_{t+j} = (a(t+j)) \bmod n = (at + aj) \bmod n = ((at) \bmod n + aj) \bmod n = (aj) \bmod n = v_j$.

That is, $v_{t+1} = v_1, v_{t+2} = v_2, \ldots, v_{t+t} = v_t = 0 = v_0$. The cycle of v_k values: $(v_0 = 0), v_1, v_2, \ldots, v_{t-1}$, consisting of t distinct elements, keeps repeating for all integers $k = t$ onward. That means, for $i \in \mathbb{Z}_n$, values v_i consist of this $t = n/g$ sized cycle repeated g times.

We can now conclude that set A contains $t = n/g$ elements. What are these elements?

Consider any element $(ai) \bmod n$. $(ai) \bmod n$ is nothing but $ai - nq$ for some integer q (Division Theorem). Since $g \mid a$ and $g \mid n$, so: $g \mid (ai - nq) \quad \Leftrightarrow \quad g \mid ((ai) \bmod n)$.

So, each element v_i of set A is a multiple of g. Also, $0 \leq v_i \leq n-1$ for any element v_i of A (they are modulo n), and there are n/g such elements. In the sequence of n consecutive integers $0, 1, 2, \ldots, n-1$ (where all v_i belong), there are total n/g multiples of g: $0, g, 2g, \ldots, ((n/g) - 1)g$.

So, the total n/g distinct elements of A, each being a multiple of g, can only be: $G = \{0, g, 2g, \ldots, ((n/g) - 1)g\}$. □

Corollary 3. *For any integers a, b, n with $n > 0$, $a \bmod n \neq 0$, and $g = gcd(a, n)$, the set of integers $A = \{(ai+b) \bmod n : i \in \mathbb{Z}_n\}$ consists of values $b, b+g, b+2g, \ldots, b+((n/g)-1)g$ after taking their mod n.*

Proof. Consider the set $A' = \{(ai) \bmod n : i \in \mathbb{Z}_n\}$ which is same as $G = \{0, g, 2g, \ldots, ((n/g) - 1)g\}$, due to Theorem 2.

For any integer $i \in \mathbb{Z}_n$, an element in set A, $(ai + b) \bmod n$, will equal $((ai) \bmod n + b) \bmod n$. But $(ai) \bmod n$ is an element in set A'. So, (considering every $i \in \mathbb{Z}_n$) all the elements of A can simply be obtained by taking all elements of A', adding b to each and taking mod n. But all elements of A' are the set G. So, set A can be obtained from set G, such that each element k in G is modified to $(k + b) \bmod n$.

Now, for any two distinct integers j and k in $\mathbb{Z}_n$, we must have $(j + b) \bmod n \neq (k + b) \bmod n$. So, modifying the elements of G (which is a subset of $\mathbb{Z}_n$) as above does not make any two of them equal. That is, A consists of same number of elements as are in G, which is n/g.

In other words, A consists of: $b, b+g, b+2g, \ldots, b+((n/g)-1)g$, all taken mod n. $\square$

Corollary 4. *For any integers a, b, n with $n > 0$, a and n coprime (i.e. $g = gcd(a, n) = 1$), the set of integers $A = \{(ai+b) \bmod n : i \in \mathbb{Z}_n\}$ is same as $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$.*

Proof. From Corollary 3, and $g = 1$, set A consists of below values after taking mod n: $b, b+1, b+2, \ldots, b+(n-1)$.

But any set of n consecutive integers, when every element is taken mod n, will give the set of integers: $\{0, 1, 2, \ldots, n-1\}$. So, set A will also be same as $\{0, 1, 2, \ldots, n-1\}$. $\square$

Corollary 5. *If n is prime, we have $g = gcd(a, n) = 1$ for all integers a. So Corollary 4 applies for all integers a when n is prime.*

We have now seen some characteristics of multiples of an integer a modulo another integer n. There is another side of this: if we are given such a multiple $(ax) \bmod n$, can we find out x? More generally, if we are given an integer $k \in \mathbb{Z}_n$, is there any integer x such that $(ax) \bmod n = k$. We will now try to understand existence of such x.

Modular Linear Equation

For given integers a, b, n with $n > 0$, $a \bmod n \neq 0$ and x unknown integer in $\mathbb{Z}_n$, the modular linear equation looks like:

$$ax \equiv b \pmod{n}$$

We need to find x, the solution of this equation where $x \in \mathbb{Z}_n$.

This equation can also be written as: $(ax - b) \bmod n = 0$. So finding x simply means that we need to find the element in set $A = \{(ai - b) \bmod n : i \in \mathbb{Z}_n\}$ which is 0 and then the corresponding i is the desired solution x. Using Corollary 3 with its b as $(-b)$, the set A consists of following values after taking their mod n: $-b, -b + g, -b + 2g, \ldots, -b + ((n/g) - 1)g$.

Let us assume that there exists some integer $m \in \{0, 1, 2, \ldots, (n/g) - 1\}$, such that a value in set A, $(-b + mg) \bmod n$, is 0. Then,

$$\begin{array}{ll} & \{\text{Such integer } m \text{ exists}\} \\ \Leftrightarrow & (-b + mg) \bmod n = 0 \\ \Leftrightarrow & (-b + mg) = kn \quad \{\text{for some integer } k\} \\ \Leftrightarrow & b/g = -kn/g + m \end{array}$$

Since $g \mid n$, if integer m exists, then b/g must be an integer, i.e. $g \mid b$.

On the other hand, if $g \mid b$ (b/g is an integer), then applying Division Theorem on integer b/g divided by integer n/g, we know that there exist integers k and m such that $0 \leq m < n/g$. That will be our desired m.

As m was the remainder in above division, so $m = (b/g) \bmod (n/g)$.

Thus we have proved this in both directions: $g \mid b$ *iff* there exists $m \in \{0, 1, 2, \ldots, (n/g) - 1\}$ such that a value in set A, $(-b + mg) \bmod n$, is 0.

To conclude, the equation has a solution *iff* $g \mid b$.

In proof of Theorem 2, we saw that the values $v_i = (ai) \bmod n$ are distinct for $i = 0, 1, 2, \ldots, t - 1$ ($t = n/g$), and then cycle for $i = t$ onward as $v_{t+j} = v_t$. Similarly, values $(ai - b) \bmod n$ will also repeat in cycles of $t = n/g$ distinct values.

So, if solutions of the equation exist, one solution x_0 must be among $\{0, 1, 2, \ldots, t-1\}$, such that $(ax_0 - b) \bmod n = 0$.

If solution x_0 exists, then for every cycle of t integers i in $\mathbb{Z}_n$, a solution must exist. There are g cycles, each of length t among i in $\mathbb{Z}_n$. So, there will be g solutions: $x = x_0 + tj$, $j = 0, 1, 2, \ldots, (n/t) - 1$.

We can write above findings in a theorem as below.

Theorem 6. *For given integers a, b, n with $n > 0$, $a \bmod n \neq 0$ and $g = gcd(a, n)$, the modular linear equation: $ax \equiv b \pmod{n}$ is solvable iff $g \mid b$. If solvable, there are total g solutions.*

Corollary 7. *For given integers a, b, n with $n > 0$, if a and n are coprime, i.e. $g = gcd(a, n) = 1$, then the equation $ax \equiv b \pmod{n}$ has exactly one solution.*

Proof. Apply Theorem 6 with $g = 1$. Since for all integers b, $1 \mid b$, so the equation is solvable and has $g = 1$ solution. □

Corollary 8. *Equation $ax \equiv 1 \pmod{n}$ is solvable iff $g = gcd(a, n) = 1$. If solvable, it has exactly one solution.*

Proof. Apply Theorem 6 with $b = 1$. Equation is solvable *iff* $g \mid 1$. That is possible only if $g = 1$. Such a solution is referred as the "Multiplicative Inverse of a modulo n", and denoted as $a^{-1} \bmod n$. □

Corollary 9. *If n is prime, $ax \equiv b \pmod{n}$ has exactly one solution, for all integers a and b.*

Proof. When n is prime, $g = gcd(a, n) = 1$, and so Corollary 7 applies. □