

Introduction to Congruences

Introduction. The study of *congruences* is fundamental in Number Theory, and its essential spirit can be captured very quickly by a simple, but important computational example: compute the least non-negative remainder that 653×107 leaves on division by 3.

Contrast these two approaches:

1. Compute the actual value of 653×107 , namely 69871, and then compute the least remainder from $69871 = 3 \times 23290 + 1$.
2. Compute the individual remainders that 653 and 107 leave on division by: $653 = 3 \times 217 + 2$, $107 = 3 \times 35 + 2$, note that $653 \times 107 = (3x + 2)(3y + 2)$ (where I have replaced the actual integers 217 and 35 by x and y), which simplifies to $3^2 xy + 2 \times 3x + 2 \times 3y + 4 = 3(3xy + 2x + 2y + 1) + 1$, and so the least remainder is 1

The important point about approach #2 is that the remainder may be computed *without* computing the *actual* value of 653×107 . This kind of device is typical of the congruence approach, as you will come to appreciate in time, and although – in these notes – you have not yet met the notion of a congruence, I will nevertheless jump ahead and express solution #2 in *congruence language/notation*:

We have $653 \equiv 2 \pmod{3}$, $107 \equiv 2 \pmod{3}$, and thus $653 \times 107 \equiv 2 \times 2 \pmod{3}$. But $2 \times 2 \equiv 1 \pmod{3}$, and so $653 \times 107 \equiv 1 \pmod{3}$, giving that 653×107 leaves remainder 1 on division by 3. And here's a second example to further illustrate the above idea: what least non-negative remainder does $2^{1,543,612,137}$ leave on division by 3? We will see that it can be calculated almost immediately, and without calculating the actual value of $2^{1,543,612,137}$. [At first it seems like magic (which, of course, it is!), but then after a while one gets a bit *blasé* about it.]

Solution. $2^2 (= 4 = 3 \times 1 + 1)$ leaves remainder 1 when divided by 3. Now, note that if one multiplies together two (or more) integers, each leaving remainder 1 when divided by 3, then the resulting number also leaves remainder 1 when divided by 3. Why? It is simple: That is because if $x_1, x_2 \in \mathbf{Z}$, and $x_1 = 3X_1 + 1$, $x_2 = 3X_2 + 1$ – and $X_1, X_2 \in \mathbf{Z}$ – then:

$$\begin{aligned} x_1 x_2 &= (3X_1 + 1)(3X_2 + 1) \\ &= 3^2 X_1 X_2 + 3X_1 + 3X_2 + 1 \\ &= 3(3X_1 X_2 + X_1 + X_2) + 1 \\ &= 3q_2 + 1, \text{ where } q_2 = 3X_1 X_2 + X_1 + X_2 \in \mathbf{Z}. \end{aligned}$$

Introduction to congruences

It follows immediately—by simply repeating that result—that if one multiplies together the integers $x_1, x_2, x_3, \dots, x_n$, where $x_i = 3X_i + 1$, $X_i \in \mathbf{Z}$ for all i with $1 \leq i \leq n$, then the product $x_1 x_2 x_3 \dots x_n$ satisfies $x_1 x_2 x_3 \dots x_n = 3q + 1$ for some $q \in \mathbf{Z}$.

Now we can immediately compute the remainder that $2^{1,543,612,137}$ leaves on division by **3** from:

$$\begin{aligned} 2^{1,543,612,137} &= \overbrace{2^2 \times 2^2 \times \dots \times 2^2}^{771,806,068 \text{ terms here}} \times 2 \\ &= (3w + 1) \times 2, \text{ (for some } w \in \mathbf{Z}) \\ &= 3w \times 2 + 2 = 3(2w) + 2 = 3W + 2, \end{aligned}$$

where $W = 2w \in \mathbf{Z}$. It follows that $2^{1,543,612,137}$ leaves remainder 2 on division by **3**.

Comment. Simple, yes? Of course it is. And a moment's reflection will show that if we replaced $2^{1,543,612,137}$ with $-2^{1,543,612,138}$, then its remainder on division by **3** would be 1, and another moment's reflection will enable us to see that the complete story – as far as division of powers of 2 by **3** is concerned – is as follows:

Simple result. For $n \in \mathbf{N}$ we have

- 2^n leaves remainder 1 on division by **3** if n is even, and
- 2^n leaves remainder 2 on division by **3** if n is odd.

Typical remainders result. If $a, b \in \mathbf{Z}$, and $a = 3A + 2$ and $b = 3B + 2$ for some $A, B \in \mathbf{Z}$, then $ab = 3C + 1$, for some $C \in \mathbf{Z}$.

Proof. We have:

$$\begin{aligned} ab &= (3A + 2)(3B + 2) \\ &= 3A \cdot 3B + 2 \times 3A + 2 \times 3B + 4 \\ &= 3(3AB + 2A + 2B + 1) + 1 \\ &= 3C + 1, \text{ for some } C \in \mathbf{Z}. \end{aligned}$$

A start on congruences. A *fundamental* point in relation to division by **3**—for example—is that it separates the integers into **3** sets of numbers:

S_0 , those leaving remainder **0** on division by **3**: $\dots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \dots$

S_1 , those leaving remainder **1** on division by **3**: $\dots, -11, -8, -5, -2, 1, 4, 7, 10, 13, \dots$

S_2 , those leaving remainder **2** on division by **3**: $\dots, -10, -7, -4, -1, 2, 5, 8, 11, \dots$

Introduction to congruences

such that if one choose a from one of these sets and b from another or the same of these sets, then the set to which their product ab belongs depends *only* on the sets to which a and b belong, and *not* on any other consideration (like, for example, the size of a and b).

So, for example, if a and b are chosen to be (the earlier) 653 and 107 (both in S_2) then their product is in the set S_2 , and the same is true if a and b are chosen, for example, to be 14 and 902

You are now ready to appreciate the following definition.

Definition. Let $m \in \mathbf{Z}$, $m \neq 0$, and let $a, b \in \mathbf{Z}$; then a and b are said to be ‘*congruent modulo m* ’ – and we write $a \equiv b \pmod{m}$ – if a leaves remainder b on division by m . In other words, a and b are congruent modulo m if: $a = mq + b$ for some $q \in \mathbf{Z}$.

Note. $a \equiv b \pmod{m}$ if and only if $m \mid (a - b)$.

Notation. If a is not congruent to b modulo m , we write $a \not\equiv b \pmod{m}$.

Examples. $16 \equiv 4 \pmod{3}$ since $16 = 3 \times 4 + 4$; alternatively $3 \mid (16 - 4)$.

$17 \equiv 2 \pmod{3}$ since $17 = 3 \times 5 + 2$; alternatively $3 \mid (17 - 5)$.

$13 \equiv 0 \pmod{3}$ since $13 = 3 \times 4 + 1$.

$18 \equiv -2 \pmod{5}$ since $18 = 5 \times 4 - 2$; alternatively $5 \mid (18 - (-2))$.

$16 \not\equiv 3 \pmod{5}$ since $5 \nmid (16 - 3)$.

$12 \not\equiv 0 \pmod{7}$ since $7 \nmid 12$.

A reason why congruences are so important. As we will shortly see, ‘congruences’ like those seen above ($16 \equiv 4 \pmod{3}$) is a *congruence*, just like ‘ $16 = 3 \times 5 + 1$ ’ is an *equation*) are(or can be thought of as being) simply a succinct way—but a highly suggestive way—of expressing work that can be done using the more familiar language of ‘remainders on division by whatever...’, but which requires more lengthy expression.

Another problem of the type seen earlier. Find the least non-negative remainder that $2^{100,001}$ leaves on division by 5.

Solution. First calculate some small powers of 2, and for each of them make a note of the remainder that each of them leaves on division by 5:

$2^1 = 2$, leaves remainder 2 on division by 5, $2^2 = 4$, leaves remainder 4 on division by 5,

$2^3 = 8$, leaves remainder 3 on division by 5, $2^4 = 16$, leaves remainder 1 on division by 5.

Introduction to congruences

That ‘1’ is going to be incredibly useful. How? Simply because of this: if a is *any* integer that leaves remainder 1 on division by 5 then a^n leaves remainder 1 on division by 5 for *every* $n \in \mathbf{N}$. How does one show that? Just by the kind of argument that you are already familiar with (from the earlier remainder work):

The details. Since $a = 5A + 1$ for some $A \in \mathbf{Z}$ then:

$$a^2 = (5A + 1)^2 = 5^2 A^2 + 2 \times 5A + 1 = 5(5A^2 + 2A) + 1 = 5B + 1, \text{ for some } B \in \mathbf{Z}.$$

Thus a^2 leaves remainder 1 on division by 5. From that one can then argue this: $a^3 = a \cdot a^2 = (5A + 1)(5B + 1) = 5(5AB + A + B) + 1 = 5C + 1$, for some $C \in \mathbf{Z}$, and so it follows that a^3 leaves remainder 1 on division by 5 as well. It should be clear that by continuing to argue in a similar fashion then one gets that *every* one of a^4, a^5, a^6, \dots leaves remainder 1 on division by 5.

Why this is so useful. Returning to our problem concerning the remainder that the number $2^{100,001}$ leaves on division by 5 we now make these simple observations: $2^{100,000} = (2^4)^{25,000}$, and so $2^{100,000}$ leaves remainder 1 on division by 5. Thus $2^{100,001} = 2 \cdot 2^{100,000} = 2(5X + 1)$, for some $X \in \mathbf{Z}$, and so we now have that:

$$2^{100,001} = 2(5X + 1) = 5(2X) + 2 = 5Y + 2, \text{ where } Y = 2X \in \mathbf{Z}.$$

Thus $2^{100,001}$ leaves remainder 2 on division by 5.

A re-statement (with explanation following) of this work in congruence notation.

Since: $2^4 \equiv 1 \pmod{5} \quad \dots \quad (i)$
then: $(2^4)^{25,000} \equiv 1^{25,000} \pmod{5} \quad \dots \quad (ii)$
and so: $2^{100,000} \equiv 1 \pmod{5} \quad \dots \quad (iii)$
then: $2 \cdot 2^{100,000} \equiv 2 \cdot 1 \equiv 2 \pmod{5} \quad \dots \quad (iv)$
and so finally, $2^{100,001} \equiv 2 \pmod{5} \quad \dots \quad (v)$

Comment/Explanation. The passage from (i) to (ii) is *like* a standard step that one does with equations (so standard that one hardly thinks about or realizes that some principle or fundamental point is involved), namely: if $A = B$ then $A^2 = B^2$, and $A^3 = B^3$, and \dots . (iii) is only a re-statement of (ii).

The passage from (iii) to (iv) is like another standard step that one does with equations namely: if $A = B$ then $2A = 2B$ (more generally: if $A = B$ then $cA = cB$, for all c). Finally, the passage from (iv) to (v) is *like* a another standard step that one does with equations (and, once again, *so* standard, that one hardly thinks it), namely: if $A = B$ and $B = C$ then $A = C$.

Introduction to congruences

What I am alluding to is that there are such *resemblance* of behaviour between equations ($a = b$, etc.) and congruences ($a \equiv b \pmod{m}$, etc.) that I wish to set them out (not all of them, just some standard, elementary ones) out, as they mark the real beginnings of our study of congruences.

Basic congruence results. In the following it is understood that m is a *non-zero* integer, and that a, b, c, \dots, A, B, C , etc. are integers.

1. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then:

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

$$a - c \equiv b - d \pmod{m} \text{ and}$$

$$ac \equiv bd \pmod{m}.$$

(In other words, just as one can **add**, **subtract** and **multiply** equations, one can do the same with congruences.

2. If $A \equiv B \pmod{m}$ and $B \equiv C \pmod{m}$ then $A \equiv C \pmod{m}$.

(This is the congruence equivalent of what one so readily does with equations: if $a = b$, and $b = c$, then $a = c$.)

3. More generally one can add or multiply *any* number of congruences:

if $a_1 \equiv b_1 \pmod{m}$, $a_2 \equiv b_2 \pmod{m}$, \dots , $a_n \equiv b_n \pmod{m}$, then

$$a_1 + a_2 + \dots + a_n \equiv b_1 + b_2 + \dots + b_n \pmod{m}, \text{ and}$$

$$a_1 \times a_2 \times \dots \times a_n \equiv b_1 \times b_2 \times \dots \times b_n \pmod{m}.$$

An important special case of #3 is:

4. If $a \equiv b \pmod{m}$ and $n \in \mathbf{N}$, then $a^n \equiv b^n \pmod{m}$.

Sample proof (I'll do the product rule). Since $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a = mq_1 + b$ and $c = mq_2 + d$, for some $q_1, q_2 \in \mathbf{Z}$. Thus:

$$\begin{aligned} ac &= (mq_1 + b)(mq_2 + d) = m^2q_1q_2 + mq_1d + mq_2b + bd \\ &= m(mq_1q_2 + q_1d + q_2b) + bd = mq_3 + bd, \end{aligned}$$

where $q_3 = mq_1q_2 + q_1d + q_2b \in \mathbf{Z}$. Thus $ac \equiv bd \pmod{m}$.

Final comment in these notes. It is essential that you become proficient in the use of congruence technique at the earliest opportunity. Practice is the key word.