

LESSON 3: CONGRUENCE ARITHMETIC

3.1 THE DIVISION ALGORITHM

An integer can be divided by another, called the **divisor**, to produce a **quotient** and a **remainder**. For example, when 65 is divided by 11 (the divisor), the quotient is 5 and the remainder 10. Note that

$$\begin{array}{ccc} & \text{divisor} & \text{remainder} \\ & \downarrow & \downarrow \\ 65 & = & 5 \cdot 11 + 10 \\ & \uparrow & \\ & \text{divisor} & \end{array}$$

When carrying out this process we found the *highest* multiple of 11 that is *less* than 65. This ensures that the remainder is a positive (perhaps zero) number less than 11. If we started with a negative say -65 , we can still to obtain a positive - actually *non-negative*, as it could be zero - remainder less than 11; the largest multiple of 11 less than -65 is -66 so

$$-65 = (-6)11 + 1$$

The Division Algorithm : Let m be any *integer* and n a *natural number*. Then m can be divided by n to obtain a quotient q and remainder r . More precisely, $m = qn + r$ where $0 \leq r < n$

3.2 THE NUMBERS $qn + r$

The remainder is zero when **n is a factor of m** (which is the same as saying **m is a multiple of n**). And then $m = qn$ where q is an integer. Alternatively n is a factor of m if $\frac{m}{n}$ is an integer. **We write $n|m$ to mean “ n is a factor of m ”.**

3.2.1 Example

Determine all integers n which have the property that $\frac{2n^3 - n^2 - 2n + 9}{n + 1}$ is an integer.

Solution: As in the case of integers, a **polynomial** can be divided by another polynomial to obtained a **quotient** and a **remainder**, where either the remainder is 0, or the **degree** of the remainder is less than the degree of the divisor.

So we divide;

$$\begin{array}{r}
 2n^2 - 3n + 1 \\
 n + 1 \overline{) 2n^3 - n^2 - 2n + 9} \\
 \underline{2n^3 + 2n^2} \\
 -3n^2 - 2n \\
 \underline{-3n^2 - 3n} \\
 n + 9 \\
 \underline{n + 1} \\
 8
 \end{array}$$

The **equation that arises from this division is**

$$2n^3 - n^2 - 2n + 9 = (n + 1)(2n^2 - 3n + 1) + 8$$

And dividing both sides by $n + 1$ we get

$$\frac{2n^3 - n^2 - 2n + 9}{n + 1} = (2n^2 - 3n + 1) + \frac{8}{n + 1} \dots\dots\dots(1)$$

(Of course we could have arrived at this equation, immediately after the long division, as

$$\text{in } \frac{25}{9} = 2 + \frac{7}{9})$$

Let's get back to the question, which is to identify all the integers n for which the fraction is an integer. Now the first term is **always** an integer, whenever n is an integer. So we need to find the integers n for which $\frac{8}{n + 1}$ is an integer. This happens only when $n + 1$ is a factor of 8!. The factors of 8 are

1, -1, 2, -2, 4, -4, 8, -8. These are only values for $n + 1$. So $n = 0, -2, 1, -3, 3, -5, 7,$ and -9 .

We capture the **process used in solving the above problem in the following.**

3.2.2 To solve a problem that requires us to determine all integers for which the fraction $\frac{f(n)}{an + b}$ is an integer,

- 1. Long divide to get remainder r to be a natural number**
- 2. Then equate $an + b$ to be equal to each factor of r and solve for n .**

The multiples of n are $0, \pm n, \pm 2n, \pm 3n, \dots$.

Consider the numbers $1, n + 1, 2n + 1, 3n + 1, \dots$. For example, for $n = 4$, the numbers are $1, 5, 9, 13, \dots$. If these numbers are divided by 4 , we see that **all leave a remainder of 1**.

So any number of the form $qn + 1$ leaves a remainder of 1 when divided by n .

3.2.3 Integers of the form $qn + r$, where $0 \leq r < n$, are precisely the numbers that leave a remainder of r when divided by n .

Examples:

1. Any number of the form $2n + 1$, where n is an integer, leaves a remainder of 1 when divided by 2. These numbers are precisely the **odd numbers**;

An integer is odd if it can be written in the form $2n + 1$ where n is an integer.

Another way of saying this is;

An integer m is odd if there exists an integer n such that $m = 2n + 1$

2. Any number of the form $6n + 5$, **where n is an integer**, when divided by 6, leaves a remainder of 5 when divided by 6.

(Check: -7, -1, 5, 11, 17, 23,....all leave a remainder of 5 when divided by 6)

3.3 CONGRUENCES MODULO 6

Recall the last example;

Any number of the form $6n + 5$, where n is an integer, when divided by 6, leaves a remainder of 5. **(Check: -7, -1, 5, 11, 17, 23,....all leave a remainder of 5 when divided by 6.)**

Let us study the above example in greater detail; we look at **all** the remainders, namely 0, 1, 2, 3, 4 and 5, and ask, "Which integers leave remainder r ($r = 0, 1, 2, 3, 4, 5$) when divided by 6?"

Remainder 0: ...-12, -6, 0, 6, 12, 18, ...

Remainder 1: ...-11, -5, 1, 7, 13, 19,

Remainder 2: ...-10, -4, 2, 8, 14, 20, ...

Remainder 3: ...-9, -3, 3, 9, 15, 21, ...

Remainder 4: ...-8, -2, 4, 10, 16, 22, ...

Remainder 5: ...-7, -1, 5, 11, 17, 23, ... (This is the example above)

For convenience, we refer to these six sets as group 0, group 1, group 2 and so on.

1. Group r contains the remainder r for each of the six values of r
2. In each group the numbers increase by 6 at each stage. Another way of saying this is that **the difference between any two numbers in a group is a multiple of 6.**

Definition: Two integers are said **congruent modulo 6** if any one of the following holds:

1. Their difference is a multiple of 6 or
2. They are in the same group, which happens when they leave the same remainder when divided by 6.

When this happens we write

$$a \equiv b \pmod{6} \text{ OR } a \equiv_6 b .$$

We read the above as “ a is congruent to b mod 6” or “mod 6, $a \equiv b$ ”.

For example,

$$47 \equiv_6 113$$

since the difference between 47 and 113 is $113 - 47 = 66 = 6 \cdot 11$ is a multiple of 6. Note that both 47 and 113 leave a remainder of 5 on division by 6, so both these numbers are in group 5

All the numbers in the same group are congruent to each other. For example, mod 6,

$$\dots - 10 \equiv_6 (-4) \equiv_6 2 \equiv_6 8 \equiv_6 14 \dots$$

3. Clearly there is nothing special about 6. We can do the same for any **positive integer** n .

3.4 CONGRUENCE MODULO n

3.4.1 Definition: Let n be any natural number. Two integers a and b are said to be congruent modulo n if either of the following conditions hold;

- (a) $a - b$ is a multiple of n , that is $n \mid a - b$ OR
- (b) a and b leave the same remainder when divided by n .

We then write

$$a \equiv b \pmod{n} \text{ OR } a \equiv_n b$$

.9 for

3.4.2 $a \equiv_n 0$ if and only if n is a factor of a , that is, a is a multiple of n .

Examples:

- (a) $n \equiv_2 0$ for any even number n and $n \equiv_2 1$ for any odd number n .
- (b) For any integer m , $mn \equiv_n 0$
- (c) If an integer n ends in 5 or 0, $n \equiv_5 0$
- (d) If u is the unit digit of a positive integer n then $n \equiv_{10} u$

If a leaves the remainder r when divided by n , then $a \equiv r \pmod n$ (for in this case, $a - r$ is a multiple of n)

3.5 PROPERTIES OF \equiv

In what follows, we take any natural number n and “fix” it. So in this paragraph “ n ” remains the same throughout. So, instead of writing \equiv_n we simply write \equiv .

Remarkably the congruence sign \equiv behaves very much as the $=$ sign.

3.5.1 If $a \equiv b$ and $c \equiv d$ then

- $(a+c) \equiv (b+d)$
- $(a-c) \equiv (b-d)$
- $ac \equiv bd$
- $a^2 \equiv b^2$
- $a^m \equiv b^m$ for any $m = 1, 2, 3, 4, \dots$
- $-r \equiv_n (n-r)$ for any natural number n .

Example

Let us confirm some of the rules above for $n = 8$. (So $m \equiv n$ whenever $m - n$ is a multiple of 8.

$19 - (-5) = 24$ is a multiple of 8 so $19 \equiv 8(-5)$.

Likewise $11 - 51 = -40$ is a multiple of 8, so $11 \equiv 851$. We have $19 \equiv 8(-5)$ and $11 \equiv 851$

Now

$(19 + 11) = 30 \equiv 86$ and

$$(-5+51)=46 \equiv 86,$$

confirming $(19+11) \equiv 8(-5 + 51)$

Also

$$(19-11) = 8 \equiv 80 \text{ and}$$

$$(-5-51) = -56 \equiv 80.$$

confirming $(19-11) \equiv 8(-5 - 51)$.

$$19.11=209 \equiv 81 \text{ and}$$

$$-5.51 \equiv 8(-255) = (-256 + 1) = 8(-32)+1 \equiv 81,$$

confirming $19.11 \equiv 8(-5)(51)$

3.6 PROOFS OF DIVISIBILITY RULES

Divisibility by 2, 4, 8, 5, 25, 125

Let us use the symbol n for an arbitrary natural number and m for the last digit. For example if

$n = 4136$, then $m = 6$. Note that in this case n is the sum of 6 and a multiple of 10

($4136 = 6 + 10 \cdot 413$). Any multiple of 10 is also a multiple of 2 and hence even. That is, any number n is an even number plus the last digit. We conclude that n is even if the last digit is even, and odd if the last digit is odd.

3.6.1 A number is even if the last digit is even, and is odd if the last digit is odd.

Any multiple of 10 is also a multiple of 5. That is, any number n is a multiple of 5 plus the last digit. We conclude that n is a multiple of 5 if the last digit is a multiple of 5, and this happens only when the last digit is either 5 or 0.

3.6.2 A number is a multiple of 5 if the last digit is either 0 or 5.

Now if m denotes the number formed by the *last two digits*, for example, in $n = 4136$, m will be 36, then n is the sum of m and a multiple of 100. But $100 = 4 \cdot 25$ is a multiple of 4 as well as 25. Hence n is multiple of 4 (or 25) only when m is a multiple of 4 (or 25).

3.6.3 A number is a multiple of 4 if the number formed by the last two digits is a multiple of 4. It is a multiple of 25 if the number formed by the last two digits is a multiple of 25, that is, it is 00,

Another way of looking at the above is through congruences. For example, let us look at m , where m is the number formed by the last three digits.

Then $n - m$ is a multiple of $1000 = 8 \cdot 125$, so $n - m$ is a multiple of 8 as well as 125. That is

$$n \equiv_8 m \ \& \ n \equiv_{125} m$$

From our discussion on congruences, n and m leave the same remainders when divided by either 8 or 125. For example, when 2134687129 is divided by 4 the remainder is the same as when 29 is divided by 4, so the remainder is 1. When divided by 8, the remainder is again equal to 1 since $129 = 8 \cdot 16 + 1$. When divided by 125, the remainder is 4, since $129 = 1 \cdot 125 + 4$, and when divided 25 the remainder is also 4.

Divisibility by 3 and 9

The observation that

$$10a + b = (a + b) + 9a$$

$$100a + 10b + c = (a + b + c) + (99a + 9b)$$

$$1000a + 100b + 10c + d = (a + b + c + d) + (999a + 99b + 9c)$$

and the fact that any number can be written in the form

$$a_0 + 10a_1 + 100a_2 + 1000a_3 + \dots = a_0 + a_1 + a_2 + a_3 + \dots + 9a_1 + 99a_2 + 999a_3 + \dots$$

allows us to conclude that any number is congruent, mod 9, to the sum of its digits. As before, the number, and the number formed by adding its digits, leave the same remainder when divided by 9.

For example when the 88 digit number 1111...11111 (88 one's) is divided by 9, its remainder is the same as when $1+1+1+\dots+1 = 88$ is divided by 9. That is the remainder is 7.

For remainder 0, we have multiples. More precisely,

3.6.4 For any n , an $n+1$ digit number $a_n a_{n-1} a_{n-2} \dots a_2 a_1 a_0$ s divisible by 9 if and only if the sum $a_n + a_{n-1} + a_{n-2} + \dots + a_2 + a_1 + a_0$ of its digits is divisible by 9

The same argument can be used to conclude

3.6.5 For any n , an $n+1$ digit number $a_n a_{n-1} a_{n-2} \dots a_2 a_1 a_0$ s divisible by 3 if and only if the sum $a_n + a_{n-1} + a_{n-2} + \dots + a_2 + a_1 + a_0$ of its digits is divisible by 3

Divisibility by 11

Note the following:

$$10^{2n} = 100^n \equiv_{11} 1^n \equiv_{11} 1$$

$$10^{2n+1} \equiv_{11} 10 \equiv_{11} -1$$

Hence :

3.6.6. An even power of 10 is congruent to 1 mod 11 and an odd [power of 10 is congruent to -1 mod 11.

This observation allows us to conclude the following.

Let $a_n a_{n-1} a_{n-2} \dots a_2 a_1 a_0$ be an $(n + 1)$ digit number. Then

$$\begin{aligned} & a_n a_{n-1} a_{n-2} \dots a_2 a_1 a_0 \\ &= a_0 + 10a_1 + 100a_2 + 1000a_3 + \dots \equiv_{11} a_0 - a_1 + a_2 - a_3 + \dots \end{aligned}$$

Which is the same as:

$$a_0 + 10a_1 + 100a_2 + 1000a_3 + \dots \equiv_{11} (a_0 + a_2 + a_4 + \dots) - (a_1 + a_3 + a_5 + \dots)$$

The right hand side is the difference between “alternate sums” of the digits of the given number. In particular:

3.6.7 $a_n a_{n-1} a_{n-2} \dots a_2 a_1 a_0$ is divisible by 11 if and only if
 $(a_0 + a_2 + a_4 + \dots) \equiv_{11} (a_1 + a_3 + a_5 + \dots)$

3.6.8 Examples

Use congruences to whether 47680245 is

- (a) divisible by 9
- (b) divisible by 11.

Solution

- (a) $4 + 7 + 6 + 8 + 0 + 2 + 4 + 5 = 36 \equiv_9 0$ so the remainder is 0. So 47680245 is divisible by 9.
- (b) $(4 + 6 + 0 + 4) - (7 + 8 + 2 + 5) = -8$ which is not divisible by 11. So 47680245 is not divisible by 11. Check!

3.7 EXERCISES

1. Discuss the parity of a product, difference and sum of two integers with reference to the parity of each of the two integers. (Problem 63)
2. If m and n are both odd integers, then which of the following numbers must be even? (Problem 64)

(a) mn	(b) $m^2n + 2$
(c) $m + n + 1$	(d) $2m + 3n + 5$
(e) $2m + n$	
3. What remainder do you get when the square of an integer is divided by 4? (Problem 65)
4. Let n be a natural number. If the tens digit of n^2 is equal to 3, then what is the last digit of n^2 ? (Problem 67)
5. Neither of the two integers m and n are divisible by 3. What are the possible remainders when $m^3 + n^3$ is divided by 9? (Problem 68)
6. What is the last digit of 3^{2011} ? (Problem 69)
7. What is the remainder when $3^{2012} + 2$ is divided by 11? (Problem 70)
8. Find the remainder when 2^{100} is divided by 5. (Problem 71)
9. Find the last two digits of 6^{2012} . (Problem 72)
10. What is the second last digit when the product $1 \times 3 \times 5 \times 7 \times \dots \times 99$ is written as a number? (Problem 73)
11. Find the value of $k + l$ if k and l are positive integers and $k + l + kl = 54$. (Problem 76)
12. What is the smallest number that leaves a remainder of 3 when divided by 10 and leaves a remainder of 4 when divided by 13? (Problem 77)

13. How many positive integers n are there such that $n + 3$ divides into $n^2 + 7$ without remainder? (Problem 78)
14. For which one of the following statements does there exist an x which makes it true? (Problem 85)
- (a) $2x \equiv 3 \pmod{12}$
 - (b) $3x \equiv 7 \pmod{12}$
 - (c) $6x \equiv 11 \pmod{12}$
 - (d) $5x \equiv 9 \pmod{12}$
 - (e) $10x \equiv 5 \pmod{12}$
15. Prove that every Pythagorean triple contains at least one multiple of each of 3, 4 and 5. (Problem 793)

3.8 PARITY

The **even** integers are

.....-6, -4, -2, 0, 2, 4, 6,

The **odd** integers are

.....-5, -3, -1, 1, 3, 5, ...

Parity is the property of an integer to be even or odd.

So two integers **have the same parity** if both are even or both are odd. It immediately follows that the **sum of two integers having the same parity is always even**. From this it immediately follows that **if the sum of two integers is odd, they have opposing parities**.

This rule does not apply to products; **the product of odd integers is odd and the product of even integers is even**.

These observations lead us to newer ones;

The sum of any set of integers, all of which are even, is even.

The sum of an even number of integers, all of which are odd, is even.

The sum of an odd number of integers, all of which are odd, is odd.

If the sum of a set of integers is even, there is an even number of odd integers in the sum.

If the sum of a set of integers is odd, there is an odd number of odd integers in the sum.

If the product of a set of integers is odd, all the numbers in the set are odd.

If the product of a set of integers is even, at least one of the numbers in the set is even

For example, it is impossible to find 5 odd numbers that add up to 100, because the sum of every 5 odd numbers is an odd.

Very useful is the fact that **a number is even when it is congruent to 0 mod 2 and odd when it is congruent to 1 mod 2**. And also that mod 2, $1 + 1 = 0$.

3.9 EXERCISES

1) Prove that the sum of two odd numbers is even and the product of two odd numbers is odd. (Problem 142)

2) Show that if the sum of two integers is odd then their product is even. (Problem 142)

3) Katya and her friends stand in a circle. It turns out that both neighbours of each child are of the same gender. If there are five boys in the circle, how many girls are there? (Problem 147)

4) Can one make change of a 25 cent coin, using in all, ten coins each having a value of 1, 3, or 5 cents? (Problem 145)

5) Given two integers a and b , consider the number $ab(a - b)$. Can you determine if it is even or odd? (Problem 146)

6) On a chessboard, a knight starts from square a_1 , and returns there after making several moves. Show that the knight makes an even number of moves. (a_1 is the bottom left corner square in a chessboard). (Problem 144)

7) There are 100 soldiers in a detachment, and every evening three of them are on duty. Can it happen that after a certain period of time each soldier has shared duty with every other soldier exactly once? (Problem 143)

8) Seven gears are placed on a plane, arranged in a circular chain. Can all the gears rotate simultaneously? (Problem 148)