Worksheet 4.1 and 4.2

Max's Lecture
MATH 54

July 2, 2019

Exercise A (from Charles). Let a, b, c be integers. If $a|bc$, is it the case that a must divide b or c?

On previous worksheet.

Exercise B(from Ritvik). Prove that if a is any integer other than 0, can you think of a number that divides a? Can you think of a number that a must divide?

On previous worksheet.

Exercise C. What are the quotient and remainder when 11 is divided by 4? What if -25 is divided by 4?

On previous worksheet.

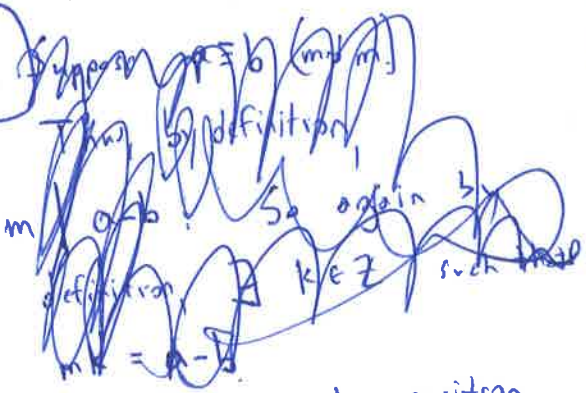
Not, I accidentally did part 2 first.

Exercise D. 4.1.21,22 Let m be a positive integer. Prove the following:

1. Let m be a positive integer. Show that $a \equiv b(\mod m)$ if $a \mod m = b \mod m$.
2. Show that $a \mod m = b \mod m$ if $a \equiv b(\mod m)$.

Together, these two prove Theroem 2 in section ~~4.1~~

2.



We will do this by contrapositive.

Suppose $a \bmod m \neq b \bmod m$

Thus, a and b have different remainders when divided by m.

Using division algorithm, we write

$a = q_1 m + r_1$ where

$b = q_2 m + r_2$

$q_1, q_2, r_1, r_2 \in \mathbb{Z}$, $0 \leq r_1, r_2 < m$

and $r_1 \neq r_2$.

We now consider

$a - b = q_1 m + r_1 - (q_2 m + r_2) =$

$m(q_1 - q_2) + r_1 - r_2$. So $a - b \equiv r_1 - r_2 \pmod m$

Since $r_1 \neq r_2$ and $-m < r_1 - r_2 < m$

You can do some case work to show this,

We can see that $r_1 - r_2 \not\equiv 0 \pmod m$.

So $a - b \not\equiv 0 \bmod m$.

as desired.

1.

We can do a direct proof of this.

Suppose ~~$a = b$ for some $a, b \in \mathbb{Z}$~~ $a \bmod m = b \bmod m$. Thus, $a - b$ have the same remainder when divided by m.

Using the division algorithm, we write $a = q_1 m + r$

$b = q_2 m + r$

where $q_1, q_2, r \in \mathbb{Z}$, $0 \leq r < m$.

We now consider

$a - b = (q_1 m + r) - (q_2 m + r)$

$= m(q_1 - q_2)$

So $m \mid a - b$. Thus, by definition of modular congruence, $a \equiv b \pmod m$, as desired.

Exercise E (4.1.45). Show that if m is a positive integer of the form $4k + 3$ for some nonnegative integer k, then m is not the sum of the squares of two integers.

The contrapositive of this is proved on the practice mid term.

$2^4 \bmod 3$ is 1.

Exercise F. Are the following true? Prove or disprove. In all cases, a, b, c, d are integers, and m is a positive integer.

1. If $ac \equiv bc \pmod{m}$ then $a \equiv b \pmod{m}$.
2. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a^c \equiv b^d \pmod{m}$.

Neither of these are true! Counterexample for 1:

$2 \cdot 3 \equiv 4 \cdot 3 \pmod 6$, but $2 \not\equiv 4 \pmod 6$.

Counterexample for 2:
$2 \equiv 2 \bmod 3$ and $1 \equiv 4 \bmod 3$,

but $2^1 \not\equiv 2^4 \bmod 3$.

this is congruent to 2

This is congruent to 1.

Exercise G. Try doing the following computations without using a calculator:

1. 6^{81} **mod** 7
2. 3^{18} **mod** 5

1. Since $6 \equiv -1 \bmod 7$,

$6^{81} \equiv (-1)^{81} \equiv -1 \equiv 6 \bmod 7$.

So $6^{81} \bmod 7 = 6$.

2. ~~Note that $3^9 \equiv -1 \bmod 5$~~

Note that $3^2 \equiv 9 \equiv -1 \bmod 5$.

So $3^{18} \equiv (3^2)^9 \equiv (-1)^9 \equiv -1 \equiv 4 \bmod 5$

So $3^{18} \bmod 5 = 4$.

Exercise H (from charles). 1. Express 74 in base 2. Express 27 in hexidecimal.

2. Convert the binary number 10101 to base 4. Do the same for base 8. Can you guess a pattern?

1. $74 = 64 + 10 = 64 + 8 + 2$

$= 2^6 + 2^3 + 2^1 =$

$(1001010)_2$.

$27 = 16^1 + 11 \cdot 16^0$.

We use B to express 11 in hexidecimal.

5. the answer is

$(1B)_{16}$

2. Before we do this, we convert $(10101)_2$ to base 10.

(This is just one possible way, there are many ways of starting this problem)

$(1010)_2 = 2^4 + 2^2 + 2^0 = 16 + 4 + 1 = 21$.

Expressing in base 4 we get

$21 = 16 + 5 = 16 + 4 + 1 =$

$4^2 + 4^1 + 4^0 =$

$(111)_4$.

Note: This is what you get when you group together the digits in the base 2 rep in groups of 2:

(10 10 1)

1 1 1

Expressing in base 8, we get

$21 = 2 \cdot 8 + 5 = 2 \cdot 8^1 + 5 \cdot 8^0 =$

$(25)_8$.

Note: This is what you get when group together the digits in the base 2 rep in groups of 3:

(10 101)

2 5

Exercise I. Suppose that an integer is expressed in the standard decimal notation. How can you tell whether the number is divisible by 3? Why does your rule work?

It turns out that a number is divisible by 3 if and only if the sum of its digits is divisible by 3.

To see this, let

$n = (d_k d_{k-1} \dots d_1 d_0)_{10}$ Then,

$$n = d_k 10^k + \dots d_1 \cdot 10^1 + d_0 \cdot 10^0$$

Since $10 \equiv 1 \pmod 3$,

$$n \equiv d_k 10^k + \dots + d_0 10^0 \equiv d_k + d_{k-1} + \dots + d_0 \pmod 3$$

From this, we see that $n \equiv 0 \pmod 3$ (aka n is divisible by 3) precicely when the sum of its digits is divisible by 3