MST125 TMA01

William B. Sørensen

December 4, 2022

1 Question 1

Contents

1.1 a

MST125 TMA 01 Question 1
William Bjørn Sørensen, I220215X
LaTeX

1.2 b

1. The distance between A($x_1,\ y_1$) and B($x_2,\ y_2$) is given by

$$\mathrm{AB} = \sqrt{\left(x_2 - x_1\right)^2 + \left(y_2 - y_1\right)^2}.$$

Hence the distance between A$(-3,\ 1)$ and B$(2,\ -2)$ is

$$\begin{aligned} \text{AB} &= \sqrt{(2-(-3))^2 + (-1-1)^2} \\ &= \sqrt{5^2 + (-3)^2} \\ &= \sqrt{34}. \end{aligned}$$

2. The gradient m of the line through $(x_1,\ y_1)$ and $(x_2,\ y_2)$ is given by

$$m = \frac{y_2 - y_1}{x_2 - x_1}.$$

Hence the gradient of the line through $(-3,\ 1)$ and $(2,\ -2)$ is

$$m = \frac{-2-1}{2-(-3)} = -\frac{3}{5}.$$

3. The gradient of the line is $-\frac{3}{5}$. Hence $\tan\alpha = -\frac{3}{5}$. Let ϕ be the acute angle that the line makes with the nagative direction of the x-axis. Then

$$\tan\phi = \frac{3}{5},$$

so

$$\phi = \tan^{-1}\left(\frac{3}{5}\right) = 0.540\ldots.$$

Hence

$$\alpha = \pi - 0.540\cdots = 2.601\ldots.$$

Therefore the angle α is 2.60 radiants (to 2 d.p.).

1.3 c

I intend to typeset my TMA through the fact that I believe the programatic power of LaTeXis a great advantage. Through MST125 I have even started using LaTeXover Markdown (with mathjax) for school assignemts now.

Using LaTeXin my daily school work leads me to a much DRYer (don't repeat yourself) documents where all my associate code can be refrenced with great accuracy without suffering from complecated compilation scripts.

I have also configured a Vim integration so I can use my primary editor for TMAs.

2 Question 2

(a) Find the least residue of 64^7 modulo 15.

$$\begin{aligned} 64^7 &\equiv x \mod 15 \\ 4^7 &\equiv x \mod 15 \end{aligned}$$

We observe $4^2 \equiv 1 \mod 15$.

$$\begin{aligned} 4^1 &\equiv x \mod 15 \\ 64^7 &\equiv 4 \mod 15 \end{aligned}$$

3 Question 3

3.1 a

3.1.1 i

We find the gcd using Euler's algorithm. These variable names come from CAS tool I wrote in Rust for Unit3.

$$\begin{array}{ccccccc} a & & q & & b & & r \\ 90 & = & 5 & \times & 17 & + & 5 \\ 17 & = & 3 & \times & 5 & + & 2 \\ 5 & = & 2 & \times & 2 & + & 1 \\ 2 & = & 2 & \times & 1 & + & 0 \end{array}$$

We reshape for substitution

$$\begin{array}{ccccccc} 5 & = & 90 & - & 5 & \times & 17 \\ 2 & = & 17 & - & 3 & \times & 5 \\ 1 & = & 5 & - & 2 & \times & 2 \end{array}$$

And then conduct said substitution

$$\begin{aligned} a \times 17 + b \times 90 &= 1 \\ &= 5 - 2 \times 2 \\ &= (90 - 5 \times 17) - 2 \times 2 \\ &= (90 - 5 \times 17) - 2 \times (17 - 3 \times 5) \\ &= (90 - 5 \times 17) - 2 \times (17 - 3 \times (90 - 5 \times 17)) \\ &= 7 \times 90 - 37 \times 17 \end{aligned}$$

Then we find the least residual of -37 and deduce that the multiplicative inverse of $17 \mod 90$ is 53.

This means the solution to $17x \equiv 9 \mod 90$ is $x \equiv 53 \times 9 \equiv 477 \equiv 27 \mod 90$.

3.1.2 ii

We begin by simplifying the congruence.

$$\begin{array}{cccccc} a & x & \equiv & b & \text{mod} & n \\ 9 & x & \equiv & 12 & \text{mod} & 90 \\ 3 & x & \equiv & 4 & \text{mod} & 30 \end{array}$$

As we can see here $\gcd(3, 30) \neq 1$ and $3 \nmid 4$ so the congruence is unsolvable.

3.1.3 iii

We begin by simplifying the congruence.

$$\begin{array}{cccccc} a & x & \equiv & b & \text{mod} & n \\ 27 & x & \equiv & 72 & \text{mod} & 90 \\ 3 & x & \equiv & 8 & \text{mod} & 10 \end{array}$$

This is small enougth for a brute force attack but for clarities sake I will not do this.

We can see they are coprime. Hence we can skip Euler's algo.

$$\begin{aligned} 10a + 3b &= 1 \\ &= 10 - 3 \times 3 \end{aligned}$$

We find least residual and multiply with 8. So $x \equiv -3 \times 8 \equiv 7 \times 8 \equiv 56 \equiv 6 \mod 10$.

3.2 b

3.2.1 i

$$7 \times 15 \equiv 105 \equiv 4 \times 26 + 1 \equiv 1 \mod 26$$

3.2.2 ii

$$\begin{array}{cccccccccc} (& 8 & + & 24 &) & \times & 15 & \equiv & 12 & \text{mod } 26 \\ (& 16 & + & 24 &) & \times & 15 & \equiv & 24 & \text{mod } 26 \\ (& 25 & + & 24 &) & \times & 15 & \equiv & 7 & \text{mod } 26 \\ (& 2 & + & 24 &) & \times & 15 & \equiv & 0 & \text{mod } 26 \end{array}$$

Using the conversion table in Figure 1 we get

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Figure 1: Linear 0-indexed α-numeric conversion table

$$\text{"IQZB"} \xrightarrow{\alpha-\text{numeric}} \{8,\ 16,\ 25,\ 2\} \xrightarrow{\text{affine}^{-1}} \{12,\ 24,\ 7,\ 0\} \xrightarrow{\alpha-\text{numeric}^{-1}} \text{"MYHA"}$$