CSCI-4116
Assignment 8

Anas Alhadi

B00895875

March 17, 2025

Question 1

Part A

gcd(237, 124):

$$\begin{array}{ccccccccc} 237 & = & 124 & \times & \underline{1} & + & \underline{113} \\ 124 & = & 113 & \times & \underline{1} & + & \underline{11} \\ 113 & = & 11 & \times & \underline{10} & + & \underline{3} \\ 11 & = & 3 & \times & \underline{3} & + & \underline{2} \\ 3 & = & 2 & \times & \underline{1} & + & \underline{1} \end{array}$$

So $gcd(237, 124) = 1$

Part B

For each step in the Euclidean algorithm, we rearrange the equation to solve for the remainder. So:

$$\begin{array}{ccccc} 113 & = & 237 & + & 124(-1) \\ 11 & = & 124 & + & 113(-1) \\ 3 & = & 113 & + & 11(-10) \\ 2 & = & 11 & + & 3(-3) \end{array}$$

We now solve for 1, subsitutting the above equations until we get the form $1 = 237x + 124y$

$$\begin{aligned}
1 &= 3 + 2(-1) \\
&= 113 + 11(-10) + (-1)[11 + 3(-3)] \\
&= 113 + 11(-11) + 3(3)
\end{aligned}$$

$$\begin{aligned}
1 &= 237 + 124(-1) + (-11)[124 + 113(-1)] + (3)[113 + 11(-10)] \\
&= 237 + 124(-12) + 113(14) + 11(-30)
\end{aligned}$$

$$\begin{aligned}
1 &= 237 + 124(-12) + (14)[237 + 124(-1)] + (-30)[124 + 113(-1)] \\
&= 237(15) + 124(-56) + 113(30)
\end{aligned}$$

$$\begin{aligned}
1 &= 237(15) + 124(-56) + (30)[237 + 124(-1)] \\
&= 237(45) + 124(-86)
\end{aligned}$$

So the $gcd(237, 124) = 237(45) + 124(-86)$

Question 2

Part A

Given $17x + 101y = 1$, we can solve for x and y via the Extended Euclidean Algorithm. So first we find the gcd(17,101) using the Euclidean Algorithm, then trace back the equations.

gcd(17,101)

$$\begin{array}{ccccccc} 101 & = & 17 & \times & \underline{5} & + & \underline{16} \\ 17 & = & 16 & \times & \underline{1} & + & \underline{1} \end{array}$$

Solving for the remainders

$$\begin{array}{ccccc} 16 & = & 101 & + & 17(-5) \end{array}$$

Solving for 1

$$\begin{array}{ccccc} 1 & = & 17 & + & 16(-1) \\ & = & 17 & + & (-1)[101 + 17(-5)] \\ & = & 17(6) & + & 101(-1) \end{array}$$

So $(x, y) = (6, -1)$

Part B

To find the inverse, we simply apply modulo 101, to the equation $1 = 17(6) + 101(-1)$. So:

$$17(6) + 101(-1) \pmod{101} = 1(\text{mod } 101)$$

$$17(6) + 0 \equiv 1(\text{mod } 101)$$

$$17(6) \equiv 1(\text{mod } 101)$$

Thus the inverse of 17 in $\mathbb{Z}/101\mathbb{Z}$ is 6

Question 3

Similar to Question 2, we: find the gcd $\rightarrow$ solve for the remainders $\rightarrow$ solve for the gcd

Part A

gcd(357, 1234)

$$\begin{array}{ccccccccc}
1234 & = & 357 & \times & \underline{3} & + & \underline{163} \\
357 & = & 163 & \times & \underline{2} & + & \underline{31} \\
163 & = & 31 & \times & \underline{5} & + & \underline{8} \\
31 & = & 8 & \times & \underline{3} & + & \underline{7} \\
8 & = & 7 & \times & \underline{1} & + & \underline{1}
\end{array}$$

Solve for the Remainders:

$$\begin{array}{ccccc}
163 & = & 1234 & + & 357(-3) \\
31 & = & 357 & + & 163(-2) \\
8 & = & 163 & + & 31(-5) \\
7 & = & 31 & + & 8(-3)
\end{array}$$

Solve for the gcd:

$$\begin{aligned}
1 &= 8 + 7(-1) \\
&= 163 + 31(-5) + (-1)[31 + 8(-3)]
\end{aligned}$$

$$\begin{aligned}
1 &= 163 + 31(-6) + 8(3) \\
&= 1234 + 357(-3) + (-6)[357 + 163(-2)] + (3)[163 + 31(-5)]
\end{aligned}$$

$$\begin{aligned}
1 &= 1234 + 357(-9) + 163(15) + 31(-15) \\
&= 1234 + 357(-9) + (15)[1234 + 357(-3)] + (-15)[357 + 163(-2)]
\end{aligned}$$

$$\begin{aligned}
1 &= 1234(16) + 357(-69) + 163(30) \\
&= 1234(16) + 357(-69) + (30)[1234 + 357(-3)]
\end{aligned}$$

$$1 = 1234(46) + 357(-159)$$

Applying modulo 1234 to both sides of the equation gives:

$$357(-159) \equiv 1(\text{mod } 1234)$$

And

$$357(1075) \equiv 1 (\text{mod } 1234)$$

So the inverse of 357 in $\mathbb{Z}/1234\mathbb{Z}$ is 1075

Part B

gcd(3125, 9987)

$$\begin{array}{ccccccc} 9987 & = & 3125 & \times & \underline{3} & + & \underline{612} \\ 3125 & = & 612 & \times & \underline{5} & + & \underline{65} \\ 612 & = & 65 & \times & \underline{9} & + & \underline{27} \\ 65 & = & 27 & \times & \underline{2} & + & \underline{11} \\ 27 & = & 11 & \times & \underline{2} & + & \underline{5} \\ 11 & = & 5 & \times & \underline{2} & + & \underline{1} \end{array}$$

Solve for the Remainders:

$$\begin{array}{ccccc} 612 & = & 9987 & + & 3125(-3) \\ 65 & = & 3125 & + & 612(-5) \\ 27 & = & 612 & + & 65(-9) \\ 11 & = & 65 & + & 27(-2) \\ 5 & = & 27 & + & 11(-2) \end{array}$$

Solve for the gcd:

$$\begin{aligned} 1 &= 11 + 5(-2) \\ &= 65 + 27(-2) + (-2)[27 + 11(-2)] \end{aligned}$$

$$\begin{aligned} 1 &= 65 + 27(-4) + 11(4) \\ &= 3125 + 612(-5) + (-4)[612 + 65(-9)] + (4)[65 + 27(-2)] \end{aligned}$$

$$\begin{aligned} 1 &= 3125 + 612(-9) + 65(40) + 27(-8) \\ &= 3125 + (-9)[9987 + 3125(-3)] + (40)[3125 + 612(-5)] + (-8)[612 + 65(-9)] \end{aligned}$$

$$\begin{aligned} 1 &= 9987(-9) + 3125(68) + 612(-208) + 65(72) \\ &= 9987(-9) + 3125(68) + (-208)[9987 + 3125(-3)] + (72)[3125 + 612(-5)] \end{aligned}$$

$$\begin{aligned} 1 &= 9987(-217) + 3125(764) + 612(-360) \\ &= 9987(-217) + 3125(764) + \ (-360)[9987 + 3125(-3)] \end{aligned}$$

$$1 = 9987(-577) + 3125(1844)$$

Applying modulo 9987 to both sides of the equation yields:

$$3125(1844) \equiv 1(\text{mod } 9987)$$

Thus the inverse of 3125 in $\mathbb{Z}/9987\mathbb{Z}$ is 1844

Question 4

The group of units mod 15 is the set:
$\{1 + 15\mathbb{Z},\ 2 + 15\mathbb{Z},\ 4 + 15\mathbb{Z},\ 7 + 15\mathbb{Z},\ 8 + 15\mathbb{Z},\ 11 + 15\mathbb{Z},\ 13 + 15\mathbb{Z},\ 14 + 15\mathbb{Z}\}$

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$2^k \pmod{14}$	1	2	4	8	$\cancel{1}$										
$4^k \pmod{14}$	1	4	$\cancel{1}$												
$7^k \pmod{14}$	1	7	4	13	$\cancel{1}$										
$8^k \pmod{14}$	1	8	4	2	$\cancel{1}$										
$11^k \pmod{14}$	1	11	$\cancel{1}$												
$13^k \pmod{14}$	1	13	4	7	$\cancel{1}$										
$14^k \pmod{14}$	1	14	$\cancel{1}$												

Thus the order of the residue classes in $G = (\mathbb{Z}/15\mathbb{Z})^*$ is:

- $Ord_G(1 + 15\mathbb{Z}) = 1$
- $Ord_G(2 + 15\mathbb{Z}) = 4$
- $Ord_G(4 + 15\mathbb{Z}) = 2$
- $Ord_G(7 + 15\mathbb{Z}) = 4$
- $Ord_G(8 + 15\mathbb{Z}) = 4$
- $Ord_G(11 + 15\mathbb{Z}) = 2$
- $Ord_G(13 + 15\mathbb{Z}) = 4$
- $Ord_G(14 + 15\mathbb{Z}) = 2$

Question 5

Part A

The subgroup generated by $2 + 17\mathbb{Z}$ is: $\{1, 2, 4, 8, 16, 15, 13, 9\}$

Part B

We are asked to find the order of $< g >$. Given that $G = (\mathbb{Z}/1237\mathbb{Z})^*$ and $g = 2 + 1237\mathbb{Z} \in G$.

1. The order of $G = \varphi(1237) = 1236$
2. We know by Lagrange's Theorem that the order of $< g >$ divides the order of G. Thus we only need to check values $e \in \{0...1236\},\ s.t\ e|1236$.

   To find the possible values of e we will need to factor 1236. Those being:

   - 1×1236
   - 2×618
   - 3×412
   - 6×206
   - 12×103
3. We know by Euler's Theorem that if the $gcd(a, m) = 1$ then $a^{\varphi(m)} \equiv 1 (\text{mod } m)$.
   Thus since $gcd(2, 1237) = 1$ we know that $2^{1236} \equiv 1 (\text{mod } 1237)$
4. Point 3. tells us that for $e = 1236$ we have $g^{1236} = 1$. We now need to test the remaing factors of 1236 to check if any satisfy the inequality $g^e = 1,\ e \in \{1, 2, 3, 4, 6, 12, 618, 412, 309, 206, 103\}$. If so the minimum value of e that satisfies it will be the orders [1].

   - $2^1 \equiv 2 (\text{mod } 1237)$
   - $2^2 \equiv 4 (\text{mod } 1237)$
   - $2^3 \equiv 8 (\text{mod } 1237)$
   - $2^4 \equiv 16 (\text{mod } 1237)$
   - $2^6 \equiv 64 (\text{mod } 1237)$
   - $2^{12} \equiv 385 (\text{mod } 1237)$
   - $2^{103} \equiv 516 (\text{mod } 1237)$
   - $2^{206} \equiv 301 (\text{mod } 1237)$
   - $2^{309} \equiv 691 (\text{mod } 1237)$
   - $2^{412} \equiv 300 (\text{mod } 1237)$
   - $2^{618} \equiv 1236 (\text{mod } 1237)$

Thus the mimimum (and only) value of e that satisfies both $g^e = 1$ and $e|Ord(G)$ is $e = 1236$
thus $Ord_G(2 + 1237\mathbb{Z}) = 1236$

[1] I used Modular Exponentiation to find the congruneces of the powers of 2

Question 6

Part A

Given $2^{122}(\text{mod } 13)$. Observe that:

1. $gcd(2,13) = 1$ so by Fermat's Theorem $2^{\varphi(13)} = 2^{12} \equiv 1(\text{mod } 13)$
2. $122 = 10(12) + 2$ so $2^{122} = (2^{12})^{10} \times 2^2$

It follows then that:

$$2^{122} \equiv (1)^{10} \times 2^2(\text{mod } 13)$$
$$2^{122} \equiv 4(\text{mod } 13)$$

Part B

Finding the last digit of a number is equivalent to applying modulo 10 to it.[2]

Given that $gcd(3,10) = 1$ then by Euler's Theorem $3^{\varphi(10)} = 3^4 \equiv 1(\text{mod } 10)$

It follows then that:

$$3^{400} = (3^4)^{100} \equiv 1^{100}(\text{mod } 10)$$
$$3^{400} \equiv 1(\text{mod } 10)$$

So the last digit is 1

[2]Kinda funny cause i didnt notice this initially but took 10 as an example to start with and only realized half way through :)