

First Assignment

Mariano D'Angelo

February 2022

Task 1

Calculate $\text{GCD}(a, b)$ and find Bezout's identity for $a=2022$, $b=752$.

rem	val	expr
r_0	2022	a
r_1	752	b
$r_2 = r_0 \bmod r_1$	518	$a - 2b$
$r_3 = r_1 \bmod r_2$	234	$b - (a - 2b) = 3b - a$
$r_4 = r_2 \bmod r_3$	50	$(a - 2b) - 2(3b - a) = 3a - 8b$
$r_5 = r_3 \bmod r_4$	34	$(3b - a) - 4(3a - 8b) = 35b - 13a$
$r_6 = r_4 \bmod r_5$	16	$(3a - 8b) - (35b - 13a) = 16a - 43b$
$r_7 = r_5 \bmod r_6$	2	$(35b - 13a) - 2(16a - 43b) = 121b - 45a$
$r_8 = r_6 \bmod r_7$	0	

The gcd of 2022 and 752 is **2**.

From the final line of the table we can see that Bezout's identity is fulfilled with **-45** for x and **121** for y.

This can be checked with: $(2022 \cdot (-45)) + (752 \cdot 121) = 2$

Task 2

Solve the following congruences:

$$\begin{aligned} 1) \quad & x + 17 = 23 \pmod{37} \quad | -17 \\ & x + 17 - 17 = 23 - 17 \pmod{37} \\ & x = 6 \pmod{37} \\ & x = \mathbf{6} \end{aligned}$$

$$\begin{aligned} 2) \quad & x + 42 = 19 \pmod{51} \quad | -42 \\ & x + 42 - 42 = 19 - 42 \pmod{51} \\ & x = -23 \pmod{51} \\ & x = -23 + 51 \pmod{51} \\ & x = 28 \pmod{51} \\ & x = \mathbf{28} \end{aligned}$$

Task 3

Solve the following congruences:

$$\begin{aligned} 1) \quad & 23^{37} \pmod{40} = \\ & 23 \cdot 23^{36} \pmod{40} = \\ & 23 \cdot 23^{12 \cdot 3} \pmod{40} = \\ & 23 \cdot 23^{4 \cdot 3 \cdot 3} \pmod{40} = \\ & 23 \cdot 23^{2 \cdot 2 \cdot 3 \cdot 3} \pmod{40} = \\ & 23 \cdot 529^{2 \cdot 3 \cdot 3} \pmod{40} = \\ & 23 \cdot (529^{2 \cdot 3 \cdot 3} \pmod{40}) \pmod{40} = \\ & 23 \cdot 9^{2 \cdot 3 \cdot 3} \pmod{40} = \\ & 23 \cdot 81^9 \pmod{40} = \\ & 23 \cdot 1^9 \pmod{40} = \mathbf{23} \end{aligned}$$

$$\begin{aligned}
2) & (-133)^{100} \bmod 10 = \\
& (-133 \bmod 10)^{100} \bmod 10 = \\
& 7^{100} \bmod 10 = \\
& 7^{4 \cdot 25} \bmod 10 = \\
& 2401^{25} \bmod 10 = \\
& 1^{25} \bmod 10 = \mathbf{1}
\end{aligned}$$

Task 4

Task 5

Assume that the Affine cipher is implemented Z_{89} , not in Z_{26} .

1. Write down encryption and decryption functions for this modification of Affine cipher.

a, b - together form the key $k(a, b)$
m - plaintext message
c - ciphertext

The encryption key is: $E_m = am + b \bmod 89$

The decryption key is: $D_c = a^{-1} \cdot (c - b)$

2. What is the number of possible keys?

The number of possible keys is: $89 \cdot \Theta(89)$ or $89 \cdot 88$. 88 is what we get from the Euler's function, following the property: $\Theta(p) = p - 1$, where p represents a prime number. This means that there is a total of 7832 possible keys.

3. Suppose that modulus $p = 89$ is public. Malicious Eve intercepts two ciphertexts encrypted with the same key sent from Alice to Bob $c_1 = 1$ and $c_2 = 69$. Assume that Eve also managed to find out that the corresponding plaintexts are $m_1 = 10$ and $m_2 = 7$. Find out the encryption key and use it to encrypt message $m_3 = 13$.

Firstly, we write down the following system of equations:

$$\begin{cases} 69 = 7a + b \bmod 89 \\ 1 = 10a + b \bmod 89 \end{cases}$$

Now we can solve it and find the key $k(a, b)$.

$$\begin{cases} 69 = 7a + b \bmod 89 \mid \cdot (-1) \\ 1 = 10a + b \bmod 89 \end{cases}$$

$$\begin{cases} -69 = -7a - b \bmod 89 \\ 1 = 10a + b \bmod 89 \end{cases}$$

After this we get:

$$-69 + 1 = -7a + 10a + 0 \bmod 89$$

$$-68 = 3a \bmod 89$$

$$(-68 \bmod 89) = 3a \bmod 89$$

$$21 = 3a \bmod 89 \mid : 3$$

$$7 = a \bmod 89$$

$$a = 7 \bmod 89$$

$$a = 7$$

Now that we have a we can find b by just replacing a 's value into one of the equations in the system.

$$69 = 7 \cdot 7 + b \bmod 89$$

$$69 = 49 + b \bmod 89$$

$$69 - 49 = b \bmod 89$$

$$20 = b \bmod 89$$

$$b = 20 \bmod 89$$

$$b = 20$$

a and b make the encryption key $\mathbf{k(7, 20)}$. Knowing that $m_3 = 13$ we can insert it into the Affine encryption function $E_m = am + b \bmod 89$, knowing that $a = 7$ and $b = 20$.

The ciphertext we get is:

$$7 \cdot 13 + 20 \bmod 89 =$$

$$91 + 20 \bmod 89 =$$

$$111 \bmod 89 = 22$$

Ciphertext c_3 is **22**.

Task 6