First Assignment

Mariano D'Angelo

February 2022

Task 1

Calculate GCD(a, b) and find Bezout's identity for a=2022, b=752.

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

1) $x + 17 = 23 \pmod{37} \mid -17$
$x + 17 - 17 = 23 - 17 \pmod{37}$
$x = 6 \pmod{37}$
$x = \mathbf{6}$

2) $x + 42 = 19 \pmod{51} \mid -42$
$x + 42 - 42 = 19 - 42 \pmod{51}$
$x = -23 \pmod{51}$
$x = -23 + 51 \pmod{51}$
$x = 28 \pmod{51}$
$x = \mathbf{28}$

Task 3

Solve the following congruences:

1) $23^{37} \bmod 40 =$
$23 \cdot 23^{36} \bmod 40 =$
$23 \cdot 23^{12 \cdot 3} \bmod 40 =$
$23 \cdot 23^{4 \cdot 3 \cdot 3} \bmod 40 =$
$23 \cdot 23^{2 \cdot 2 \cdot 3 \cdot 3} \bmod 40 =$
$23 \cdot 529^{2 \cdot 3 \cdot 3} \bmod 40 =$
$23 \cdot (529^{2 \cdot 3 \cdot 3} \bmod 40) \bmod 40 =$
$23 \cdot 9^{2 \cdot 3 \cdot 3} \bmod 40 =$
$23 \cdot 81^{9} \bmod 40 =$
$23 \cdot 1^{9} \bmod 40 = \mathbf{23}$

2) $(-133)^{100}$ mod 10 =
(-133 mod 10)^{100} mod 10 =
7^{100} mod 10 =
$7^{4 \cdot 25}$ mod 10 =
2401^{25} mod 10 =
1^{25} mod 10 = **1**

Task 4

Task 5

Task 6