6 Tutorial 6 – November 7th, 2017

6.1 Find all natural numbers x, $0 \leq x < 555$ for which $233\,x \equiv 5 \pmod{555}$.

Solution. The fact that $233\,x \equiv 5 \pmod{555}$ can be reformulated as

$$233\,x = 5 + k \cdot 555, \quad \text{so} \quad 233\,x - 555\,k = 5.$$

If we substitute y for $-k$ we get the following Diophantic equation $233\,x + 555\,y = 5$. (Notice that in this case we are interested only in x, but to calculate it we need to find y as well.)

$$\begin{array}{rcrcr}
555 & = & 2 \cdot 233 & + & 89 \\
233 & = & 2 \cdot 89 & + & 55 \\
89 & = & 1 \cdot 55 & + & 34 \\
55 & = & 1 \cdot 34 & + & 21 \\
34 & = & 1 \cdot 21 & + & 13 \\
21 & = & 1 \cdot 13 & + & 8 \\
13 & = & 1 \cdot 8 & + & 5 \\
8 & = & 1 \cdot 5 & + & 3 \\
5 & = & 1 \cdot 3 & + & 2 \\
3 & = & 1 \cdot 2 & + & 1 \\
2 & = & 2 \cdot 1 & + & 0
\end{array}$$

We have obtained $\gcd(233, 555) = 1$. Moreover, 5 is one of the remainders. Therefore, it suffices to do the extended Euclid's algorithm till we get 5.

We obtain $x = 505$ (and $y = -212$). Since 233 and 555 are relative prime, $x = 505$ is the only solution $x = 505 + k\,555, k \in \mathbb{Z}$ which satisfies $0 \leq x < 555$.

Solution is $x = 505$.

6.2 In $\mathbf{Z}_{414}$ find all x for which

$$152\,x = 6.$$

6.3 In $\mathbf{Z}_{414}$ find all x for which

$$84\,x = 12.$$

6.4 Find the remainder when you divide

$$13^{742} - 10 \cdot 14^{521} + 22^{102}.$$

by 7.

Solution. We have $13 \equiv -1 \pmod{7}$, hence $13^{742} \equiv (-1)^{742} \pmod{7} \equiv 1 \pmod{7}$.

We have $14 \equiv 0 \pmod{7}$, hence $14^{521} \equiv 0^{742} \pmod{7} \equiv 0 \pmod{7}$.

We have $22 \equiv 1 \pmod{7}$, hence $^{102} \equiv 1^{102} \pmod{7} \equiv 1 \pmod{7}$.

Therefore, the remainder of the division is the same as the remainder of $1 - 10' \cdot 0 + 1 = 2$.

Answer: The remainder equals 2.

6.5 Find the remainder when you divide

$$4^{254} + 2 \cdot 7^{123} - 3 \cdot 11^{102}.$$

by 5.

6.6 Derive and prove criteria for divisibility by 7 and 11.

6.7 Write down the multiplication table for $(\mathbb{Z}_{10}, \odot)$.

6.8 Find all invertible elements in $(\mathbb{Z}_{11}, \odot)$ and their inverses.

Solution. Invertible elements of $\mathbb{Z}_{11}$ are all classes $[i]_{11}$ for which i and 11 are relatively prime and $0 \leq i < 11$. Since 11 is a prime number, they are all nonzero elements of $\mathbb{Z}_{11}$. Hence the set of all invertible elements is

$$\{[1]_{11}, [2]_{11}, [3]_{11}, \ldots, [9]_{11}, [10]_{11}\}.$$

Moreover,

- $[1]_{11}^{-1} = [1]_{11}$.
- Because $[2]_{11} \odot [6]_{11} = [1]_{11}$, we have $[2]_{11}^{-1} = [6]_{11}$ and $[6]_{11}^{-1} = [2]_{11}$.
- Because $[3]_{11} \odot [4]_{11} = [1]_{11}$, we have $[3]_{11}^{-1} = [4]_{11}$ and $[4]_{11}^{-1} = [3]_{11}$.
- Because $[5]_{11} \odot [9]_{11} = [1]_{11}$, we have $[5]_{11}^{-1} = [9]_{11}$ and $[9]_{11}^{-1} = [5]_{11}$.
- Because $[7]_{11} \odot [8]_{11} = [1]_{11}$ we have $[7]_{11}^{-1} = [8]_{11}$ and $[8]_{11}^{-1} = [7]_{11}$.
- Finally, $[10]_{11} \odot [10]_{11} = [1]_{11}$, $[10]_{11}^{-1} = [10]_{11}$.

6.9 Find all invertible elements in $(\mathbb{Z}_{12}, \odot)$ and their inverses.

Answers

6.2 There are two solutions, namely $x_1 = 30$, and $x_2 = 237$.

6.3 There are six solutions, namely $x_1 = 10$, $x_2 = 79$, $x_3 = 148$, $x_4 = 217$, $x_5 = 286$, and $x_6 = 355$.

6.5 The remainder equals 4.

6.7 The table is

$\odot$	$[0]_{10}$	$[1]_{10}$	$[2]_{10}$	$[3]_{10}$	$[4]_{10}$	$[5]_{10}$	$[6]_{10}$	$[7]_{10}$	$[8]_{10}$	$[9]_{10}$
$[0]_{10}$	$[0]_{10}$	$[0]_{10}$	$[0]_{10}$	$[0]_{10}$	$[0]_{10}$	$[0]_{10}$	$[0]_{10}$	$[0]_{10}$	$[0]_{10}$	$[0]_{10}$
$[1]_{10}$	$[0]_{10}$	$[1]_{10}$	$[2]_{10}$	$[3]_{10}$	$[4]_{10}$	$[5]_{10}$	$[6]_{10}$	$[7]_{10}$	$[8]_{10}$	$[9]_{10}$
$[2]_{10}$	$[0]_{10}$	$[2]_{10}$	$[4]_{10}$	$[6]_{10}$	$[8]_{10}$	$[0]_{10}$	$[2]_{10}$	$[4]_{10}$	$[6]_{10}$	$[8]_{10}$
$[3]_{10}$	$[0]_{10}$	$[3]_{10}$	$[6]_{10}$	$[9]_{10}$	$[2]_{10}$	$[5]_{10}$	$[8]_{10}$	$[1]_{10}$	$[4]_{10}$	$[7]_{10}$
$[4]_{10}$	$[0]_{10}$	$[4]_{10}$	$[8]_{10}$	$[2]_{10}$	$[6]_{10}$	$[0]_{10}$	$[4]_{10}$	$[8]_{10}$	$[2]_{10}$	$[6]_{10}$
$[5]_{10}$	$[0]_{10}$	$[5]_{10}$	$[0]_{10}$	$[5]_{10}$	$[0]_{10}$	$[5]_{10}$	$[0]_{10}$	$[5]_{10}$	$[0]_{10}$	$[5]_{10}$
$[6]_{10}$	$[0]_{10}$	$[6]_{10}$	$[2]_{10}$	$[8]_{10}$	$[4]_{10}$	$[0]_{10}$	$[6]_{10}$	$[2]_{10}$	$[8]_{10}$	$[4]_{10}$
$[7]_{10}$	$[0]_{10}$	$[7]_{10}$	$[4]_{10}$	$[1]_{10}$	$[8]_{10}$	$[5]_{10}$	$[2]_{10}$	$[9]_{10}$	$[6]_{10}$	$[3]_{10}$
$[8]_{10}$	$[0]_{10}$	$[8]_{10}$	$[6]_{10}$	$[4]_{10}$	$[2]_{10}$	$[0]_{10}$	$[8]_{10}$	$[6]_{10}$	$[4]_{10}$	$[2]_{10}$
$[9]_{10}$	$[0]_{10}$	$[9]_{10}$	$[8]_{10}$	$[7]_{10}$	$[6]_{10}$	$[5]_{10}$	$[4]_{10}$	$[3]_{10}$	$[2]_{10}$	$[1]_{10}$

6.9 Invertible elements are: $[1]_{12}$, $[5]_{12}$, $[7]_{12}$, and $[11]_{12}$. We have: $[1]_{12}^{-1} = [1]_{12}$, $[5]_{12}^{-1} = [5]_{12}$, $[7]_{12}^{-1} = [7]_{12}$, and $[11]_{12}^{-1} = [11]_{12}$