Modular arithmetic - exercises

1. Use the Euclidean algorithm to find $\gcd(a, b)$ and express it as an linear combination of a and b with integer coefficients in each of the following cases:

   a) $a = 54$, $b = 135$.

   b) $a = 21$, $b = 111$.

   c) $a = 253$, $b = 713$.

2. List all elements of the sets $\mathbb{Z}_7$, $\mathbb{Z}_7^*$, $\mathbb{Z}_8$, and $\mathbb{Z}_8^*$.

3. Use the Euclidean algorithm to find the multiplicative inverse of:

   a) 7 in $\mathbb{Z}_{31}^*$.

   b) 7 in $\mathbb{Z}_{137}^*$.

   c) 29 in $\mathbb{Z}_{431}^*$.

4. Solve the congruences:

   a) $3x \equiv 5 \pmod{31}$.

   b) $5x \equiv 2 \pmod{11}$.

5. Solve the systems of congruences:

   a) $\begin{cases} x \equiv 4 \pmod{6}, \\ x \equiv 5 \pmod{35}. \end{cases}$

   b) $\begin{cases} x \equiv 7 \pmod{7}, \\ x \equiv 1 \pmod{19}. \end{cases}$

   c) $\begin{cases} x \equiv 2 \pmod{3}, \\ x \equiv 1 \pmod{5}, \\ x \equiv 4 \pmod{11}. \end{cases}$

   d) $\begin{cases} x \equiv 38 \pmod{103}, \\ x \equiv 81 \pmod{83}, \\ x \equiv 3 \pmod{95}. \end{cases}$

6. Determine the order of:

   a) $\mathbb{Z}_8^*$.

   b) $\mathbb{Z}_9^*$.

   c) $\mathbb{Z}_{14}^*$.