Zestaw 10

1. Wskaż $a \in \mathbb{Z}$ takie, że

[(a)]$a \equiv 4 \pmod 6$, $a \equiv 5 \pmod{35}$, $4a \equiv 1 \pmod{31}$, $2a \equiv 6 \pmod{13}$.

2. Wykorzystując algorytm Euklidesa, znajdź element odwrotny do k w $\mathbb{Z}_n$, gdzie:

[(a)]$n = 42$, $k = 8$, $n = 43$, $k = 8$, $n = 73$, $k = 14$, $n = 83$, $k = 11$.

3. Oblicz wartość funkcji Eulera dla następujących liczb:
17, 49, 210, 2^8, $73 \cdot 79$, $47 \cdot 5$.

4. Wykonaj podane potęgowania w $\mathbb{Z}_n$:

[(a)]5^{16}, $n = 17$, 4^{120}, $n = 11 \cdot 13$, 2^{10}, $n = 5$, 12^7, $n = 7$.

5. Znajdź rozwiązania równań:

[(a)]$x^2 \equiv 2 \pmod 7$, $x^2 \equiv 6 \pmod{19}$.

6. Stosując metodę RSA dla podanych p i q, zaszyfruj l i odszyfruj m.

[(a)]$p = 5$, $q = 3$, $e = 7$, $l_1 = 10$, $l_2 = 7$ (odp.: $m_1 = 10$, $m_2 = 13$), $p = 17$, $q = 5$, $e = 13$, $l_1 = 27$, $l_2 = 14$, $l_3 = 32$ (odp.: $m_1 = 62$, $m_2 = 39$, $m_3 = 2$), $p = 11$, $q = 23$, $e = 17$, $l_1 = 16$, $l_2 = 8$, $l_3 = 32$ (odp.: $m_1 = 234$, $m_2 = 13$, $m_3 = 164$), $p = 11$, $q = 23$, $e = 31$, $l_1 = 234$, $l_2 = 13$, $l_3 = 164$ (odp.: $m_1 = 36$, $m_2 = 233$, $m_3 = 87$).