Kryptografia z elementami algebry

Ćwiczenia 4, Grupa ilorazowa, twierdzenie o izomorfizmie

1. Wyznacz elementy grupy ilorazowej $\Phi(21)/H$ i utworzyć tabelkę działań w tej grupie, gdzie $H = \{1, 8, 13, 20\}$.

2. Wyznacz elementy grupy ilorazowej $\mathbb{Z}_{12}^{+}/H$ i utworzyć tabelkę działań w tej grupie, gdzie $H = \{0, 4, 8\}$.

3. Wyznacz elementy grupy ilorazowej $\mathbb{Z}^{+}/5\mathbb{Z}^{+}$ i utworzyć tabelkę działań w tej grupie.

4. Niech $E : Y^2 = X^3 + 2X + 3$ nad $\mathbb{F}_7$.

   (a) Wyznacz $H = \langle P \rangle$, gdzie $P = (3, 6)$, $P \in E(\mathbb{F}_7)$.

   (b) Oblicz $\mathrm{ord}(Q)$, gdzie $Q = (6, 0)$, $Q \in E(\mathbb{F}_7)$.

   (c) Wyznacz elementy grupy ilorazowej $E(\mathbb{F}_7)/\langle Q \rangle$. Utworzyć tabelkę działań w tej grupie.

5. Niech $E : Y^2 = X^3 + 2X + 3$ nad $\mathbb{F}_7$, $S \in E(\mathbb{F}_7)$, gdzie $S = (2, 1)$, $\mathrm{ord}(S) = 6$. Udowodnij, że

$$\mathbb{Z}^{+}/6\mathbb{Z}^{+} \cong E(\mathbb{F}_7).$$

   Rozważ odwzorowanie,

$$\varphi : \mathbb{Z}^{+} \to E(\mathbb{F}_7), \qquad n \mapsto nS$$

6. Niech $E : Y^2 = X^3 + 2X + 3$ nad $\mathbb{F}_7$, $P, Q \in E(\mathbb{F}_7)$, gdzie $S = (6, 0)$, $P = (3, 6)$. Udowodnij, że

$$\mathbb{Z}_3^{+} \cong E(\mathbb{F}_7)/\langle Q \rangle$$

   Rozważ odwzorowanie,

$$\varphi : \mathbb{Z}_3^{+} \to E(\mathbb{F}_7)/\langle Q \rangle, \qquad n \mapsto n(P + \langle Q \rangle)$$