

ALGEBRA II
ZESTAW 3
ZASTOSOWANIE TEORII PODZIELNOŚCI W TEORII LICZB

1. Sprawdzić, czy kongruencja $x^2 \equiv a \pmod{n}$ posiada rozwiązanie.

- (1) $a = 29, p = 43$.
- (2) $a = 93, p = 137$.
- (3) $a = 221, p = 383$.
- (4) $a = 1801, p = 8191$.
- (5) $a = 14993, p = 65537$.

2. Dla jakich liczb pierwszych p wielomiany $X^2 + 1$ oraz $X^2 + X + 1$ są nierozkładalne nad $\mathbb{Z}_p$?

3. Niech $p \in \mathbb{P}$.

- (1) Udowodnić, że istnieją $x, y \in \mathbb{Z}$ takie, że $p = x^2 - 3y^2$ wtedy i tylko wtedy, gdy $p \equiv 1 \pmod{12}$.
- (2) Udowodnić, że istnieją $x, y \in \mathbb{Z}$ takie, że $p = -x^2 + 3y^2$ wtedy i tylko wtedy, gdy $p = 2, 3$ lub $p \equiv 11 \pmod{12}$.
- (3) Udowodnić, że istnieją $x, y \in \mathbb{Z}$ takie, że $p = x^2 - 6y^2$ wtedy i tylko wtedy, gdy $p = 3$ lub $p \equiv 1, 19 \pmod{24}$.
- (4) Udowodnić, że istnieją $x, y \in \mathbb{Z}$ takie, że $p = -x^2 + 6y^2$ wtedy i tylko wtedy, gdy $p = 2$ lub $p \equiv 5, 23 \pmod{24}$.

4. Niech $p \in \mathbb{P}, p \equiv 3 \pmod{4}$. Udowodnić, że $2p + 1 \in \mathbb{P}$ wtedy i tylko wtedy, gdy $2p + 1 \mid 2^p - 1$.

5. Niech $p \in \mathbb{P}, p \neq 2, 5$. Udowodnić następujące wzory.

- (1) $\left(\frac{5}{p}\right) = \begin{cases} 1 & p \equiv 1, 4 \pmod{5}, \\ -1 & p \equiv 2, 3 \pmod{5}, \end{cases}$
- (2) $\left(\frac{-5}{p}\right) = \begin{cases} 1 & p \equiv 1, 3, 7, 9 \pmod{20}, \\ -1 & p \equiv 11, 13, 17, 19 \pmod{20}. \end{cases}$

6. Jeśli $p \in \mathbb{P}, p \neq 2, 7$, to

- (1) $\left(\frac{7}{p}\right) = \begin{cases} 1 & p \equiv 1, 3, 9, 19, 25, 27 \pmod{28}, \\ -1 & p \equiv 5, 11, 15, 17, 23 \pmod{28}, \end{cases}$
- (2) $\left(\frac{-7}{p}\right) = \begin{cases} 1 & p \equiv 1, 2, 4 \pmod{7}, \\ -1 & p \equiv 3, 5, 6 \pmod{7}. \end{cases}$

7. Znaleźć wszystkie $x, y \in \mathbb{Z}$ spełniające następujące warunki.

- (1) $x^2 + 3 = y^2$.
- (2) $4x^2 + 4x + 4 = y^2$.
- (3) $x^2 + x + 1 = y^2$.
- (4) $x^3 - 1 = y^2$.