Warsztaty KFnrD, *Równania diofantyczne*, Lista 3, 8.12.2019 (niedziela)

Mówimy, że pierścień R jest *dziedziną* (*całkowitości*), gdy dla każdych $x, y \in R \setminus \{0\}$ mamy $xy \neq 0$.

(1) Załóżmy, że pierścień R jest dziedziną oraz $r, s \in R$. Udowodnić, że następujące warunki są równoważne:
  (a) istnieje $u \in R^*$, taki że $s = ur$;
  (b) $r|s$ i $s|r$.

(2) Niech R będzie dziedziną z jednoznacznością rozkładu na elementy nierozkładalne. Załóżmy, że $x, y \in R \setminus \{0\}$ są względnie pierwsze oraz istnieje $z \in R$, taki że $xy = z^2$. Udowodnić, że istnieją $v, w \in R$ oraz $u, u' \in R^*$, takie że:

$$x = uv^2, \qquad y = u'w^2.$$

(3) Udowodnić, że:
  (a) w pierścieniu $\mathbb{Z}[\sqrt{-5}]$ mamy równość:

$$2 \cdot 3 = \left(1 + \sqrt{-5}\right) \cdot \left(1 - \sqrt{-5}\right);$$

  (b) elementy $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ są nierozkładalne w pierścieniu $\mathbb{Z}[\sqrt{-5}]$;
  (c) pierścień $\mathbb{Z}[\sqrt{-5}]$ nie ma własności jednoznacznego rozkładu na elementy nierozkładalne;
  (d) element 2 nie jest pierwszy w pierścieniu $\mathbb{Z}[\sqrt{-5}]$.

  Wskazówka: Zadanie (5) z Listy 1 i Zadanie (4) z Listy 2.

(4) Udowodnić, że mamy następującą równość ideałów w pierścieniu $\mathbb{Z}[\sqrt{-5}]$:

$$(3) = (3, 1 + \sqrt{-5}) \cdot (3, 1 - \sqrt{-5}).$$

(5) Udowodnić, że pierścienie $\mathbb{Z}$ i $\mathbb{Z}[i]$ są pierścieniami ideałów głównych.
  Wskazówka: w obu sytuacjach udowodnić, że generatorem danego niezerowego ideału jest jego niezerowy element o najmniejszej wartości bezwględnej.

(6) Udowodnić, że ideał $(2, X)$ **nie** jest główny w pierścieniu $\mathbb{Z}[X]$.

(7) Rozważmy krzywą $E \subset \mathbb{R}^2$ daną równaniem:

$$Y^2 = X^3 + 1$$

  i załóżmy, że $(x, y) \in E$ oraz $y \neq 0$.
  (a) Znaleźć równanie prostej L, która jest styczna do krzywej E w punkcie (x, y).
  (b) Udowodnić, że prosta L z podpunktu (a) przecina się z krzywą E w „nowym” punkcie o współrzędnych:

$$\left(\frac{x^4 - 8x}{4y^2}, \frac{-x^6 - 20x^3 + 8}{8y^3}\right)$$

  (*formuła duplikacji*).
  (c) Zauważyć, że $(2, 3) \in E$.
  (d) Udowodnić, że równanie $Y^2 = X^3 + 1$ ma nieskończenie wiele rozwiązań wymiernych.