Twierdzenie o wielomianie pierwotnym

Celemn nienjszej notki jest przedstawienie dowodu twierdzenia Gaussa.

Twierdzenie 0.1 (Gaussa) *Niech $f \in \mathbb{Z}[x]$ będzie wielomianem o współczynnikach całkowitych $f(x) = \sum_{k=0}^{n} a_k x^k$, to f jest nierozkładalny nad $\mathbb{Q}$ wtedy i tylko wtedy gdy f jest nierozkładalny nad $\mathbb{Z}$.*

Wprowadzimy pojęcie wielomianu pierwotnego.

Definicja 0.1 *Wielomian $f(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$ stopnia n jest wielomianem pierwotnym wtedy i tylko wtedy, gdy wszystkie jego współczynniki są względnie pierwsze ($NWD(a_0, \ldots, a_n) = 1$).*

Lemat 0.1 *Iloczyn dwóch wielomianów pierwotnych jest wielomianem pierwotnym.*

Dowòd. *Dowód niewprost. Niech $f = a_0 + \ldots + a_n x^n$ i $g = b_0 + \ldots + b^m x^m$ bedą wielomianami pierwotnymi dla których iloczyn $c_0 + \ldots + c_{n+m} x^{n+m}$ nie jest wielomianem pierwotnym. Więc istnieje liczba pierwsza p która dzieli wszystkie współczynniki $c_0, \ldots, c_{n+m}$. Niech $n_0 \leq n$ i $m_0 \leq m$ będą najmniejszymi liczbami naturalnymi, dla których p nie dzieli a_{n_0} i b_{m_0}. Wyznaczmy współczynnik $c_{n_0+m_0}$*

$$c_{n_0+m_0} = a_0 b_{n+m_0} + a_1 b_{n_0+m_0-1} + \ldots a_{n_0} b_{m_0} + a_{n_0+1} b_{m_0-1} + \ldots a_{n_0+m_0} b_0.$$

Zauważmy, że

$$p | c_{n_0+m_0} \wedge p | a_0 b_{n_0+m_0}, \ldots p | a_{n_0-1} b_{m_0+1}, p | a_{n_0+1} b_{m_0-1}, \ldots, p | a_{n_0+m_0} b_0,$$

więc również p dzieli $a_{n_0} b_{m_0}$, a stąd $p | a_{n_0}$ lub $p | b_{m_0}$, sprzeczność z definicją liczb n_0 i m_0. ■

Dowòd. *Twierdzenia 0.1. Jezeli wielomian jest nierozkładalny nad $\mathbb{Q}$, to oczywiście jest nierozkładalny nad $\mathbb{Z}$. W drugą stronę, załóżmy że f jest nierozkladalny nad $\mathbb{Z}$ a jest rozkładalny nad $\mathbb{Q}$. Wtedy istnieją wielomiany $h, g \in \mathbb{Q}[x]$ dla których mamy $f = gh$. Wówczas istnieją wielomiany pierwotne $g_0, h_0 \in \mathbb{Z}[x]$ oraz liczby całkowite $a, b, a', b' \in \mathbb{Z}$ takie że*

$$h = \frac{a}{b} h_0 \wedge g = \frac{a'}{b'} g_0 \wedge NWD(a, b) = 1 \wedge NWD(a', b') = 1.$$

Zauważmy że z Lematu wielomian $h_0 g_0 = c_0 + \ldots + c_n x^n \in \mathbb{Z}[x]$ jest pierwotny. Przypuśćmy że b nie dzieli a'. Niech liczba p będzie dzielnikiem pierwszym *liczby b, to istnieje liczba naturalna $k \leq n$ że p nie dzieli c_k. Ponieważ liczba $\frac{aa'}{bb'}c_k \in \mathbb{Z}$ jest liczbą całkowitą i m jest największą liczbą taką że $p^m|b$, stąd $p^m|a'$ (b i a są względnie pierwsze). Więc b dzieli a'. Analogicznie $b'|a$, więc $\frac{aa'}{bb'} \in \mathbb{Z}$ jest liczbą całkowitą, stąd ostatecznie*

$$hg = (\frac{aa'}{bb'}h_0)g_0, \quad \frac{aa'}{bb'}h_0, g_0 \in \mathbb{Z}[x]$$

jest iloczynem wielomianów o współczynnikach całkowitych, sprzeczność z założeniem że f jest nierozkładalny nad $\mathbb{Z}$. ■

Robert Rałowski