Kryterium Eisensteina

Twierdzenie 0.1 (Kryterium Eisensteina) *Niech $f \in \mathbb{Z}[x]$ będzie wielomianem o współczynnikach całkowitych $f(x) = \sum_{k=0}^{n} a_k x^k$ o takiej własności że istnieje liczba pierwsza $p \in \mathbb{N}$ taka że*

$$\neg p | a_n \wedge p | a_{n-1} \wedge \ldots \wedge p | a_0 \wedge \neg p^2 | a_0,$$

to f nie jest rozkładalny nad $\mathbb{Z}$.

Dowòd. *Przypuśćmy że teza nie zachodzi dla pewnego $f \in \mathbb{Z}[x]$ przy prawdziwych założeniach. Niech więc $f = f_1 f_2$ dla pewnych $f_1, f_2 \in \mathbb{Z}[x]$ takich że $m := st\ f_1 < st\ f\ i\ st\ f_2 < st\ f$. Niech ponadto $f_1(x) = \sum_{k=0}^{m} b_k x^k$ i $f_2(x) = \sum_{k=0}^{n-m} c_k x^k$. To wtedy $a_0 = b_0 c_0$, niech $p | b_0$ to $\neg p | c_0$, bo w przeciwnym przypadku $p^2 | a_0$ wbrew założeniu. Niech $k \in \{1, \ldots, m\}$ będzie liczbą że dla każdego $i < k$ $p | b_i$, to wtedy mamy że $k \leq m = st\ f_1 < st\ f = n$ a stąd $p | a_k$ oraz:*

$$a_k = \sum_{i=0}^{k} b_i c_{k-i} = \sum_{i=0}^{k-1} b_i c_{k-i} + b_k c_0,$$

stąd $p | b_k c_0$ (bo $p | b_i$ dla $i < k$) a stąd $p | b_k$, więc dla każdego $i \in \{0, \ldots, m\}$ $p | b_i$. Z drugiej strony mamy z założenia $\neg p | a_n$ oraz:

$$a_n = \sum_{k=0}^{n} b_k c_{n-k} = \sum_{k=0}^{m} b_k c_{n-k}$$

a stąd wynikałoby że $p | a_n$, sprzeczność z założeniem. ■

Jako zastostosowanie kryterium Eisensteina, mamy następujące twierdzenie:

Twierdzenie 0.2 *Niech $p \in \mathbb{N}$ będzie liczbą pierwszą, to wielomian $f(x) = \sum_{k=0}^{p-1} x^k \in \mathbb{Z}[x]$ jest nierozkładalny nad $\mathbb{Z}$.*

Dowòd. *Oczywiście nie możemy zastosować wprost wspomnianego wyżej kryterium, więc zastosujmy podstawienie $x = y + 1$, to wtedy:*

$$f(x) = \sum_{k=0}^{p-1} x^k = \frac{x^p - 1}{x - 1} = \frac{(y+1)^p - 1}{y} = \frac{1}{y}\left(\sum_{k=0}^{p} \binom{p}{k} y^k - 1 \right) =$$

$$= \frac{1}{y}\left(1 + \sum_{k=1}^{p} -1 \binom{p}{k} y^k \right) = \sum_{k=1}^{p} \binom{p}{k} y^{k-1} = \sum_{k=0}^{p-1} \binom{p}{k+1} y^k.$$

Zauważmy, że dla $k \in \{0, \ldots, p-1\}$ *mamy* $a_k = \binom{p}{k+1}$, *co daje fakt że dla* $k < p-1$ *współczynnik* $a_k = \frac{p!}{(k+1)!(p-(k+1))!}$ *jest liczbą całkowitą podzielną przez liczbę pierwszą* p, *natomiast dla* $k = p-1$ $a_k = \binom{p}{p} = 1$. *Mamy ponadto, że* $a_0 = \binom{p}{1} = p$, *tak więc liczba pierwsza* p *dzieli* a_0 *ale* p^2 *nie dzieli* a_0. *Więc założenia kryterium Eisensteina są spełnione dla wielomianu* $h(y) = f(y+1)$. *Kryterium te daje nierozkładalność wielomianu* h *nad* $\mathbb{Z}$ *a więc w resultacie sam wielomian* f *jest nierozkładalny nad pierścieniem* $\mathbb{Z}$. ■

Robert Rałowski