Dowody wstępne

Lemat 1. *Dla każdych liczb całkowitych nieujemmych* n, m *nie równych jednocześnie 0, o największym wspólnym dzielniku* d *istnieją liczby całkowite* k, l *takie, że* $nk + lm = d$

Dowód. Dokonajmy indukcji po sumie tych liczb. Dla sumy wynoszącej 1 mamy, że z dokładnością do permutacji $n = 1$, $m = 0$. Wtedy biorąc $k = 1$, $l = 0$ uzyskujemy prawdziwość tezy indukcyjnej.

Załóżmy więc, że teza jest prawdziwa dla wszystkich par (n, m) o sumie mniejszej niż pewne S. Rozpatrzmy dowolną parę (n, m) o sumie S. Bez straty ogólności załóżmy, że $n \geqslant m$ (co daje $n > 0$). Łatwo widać, że $d \mid n \wedge d \mid m \iff d \mid n - m \wedge d \mid m$, czyli największy wspólny dzielnik liczb (n, m) to największy wspólny dzielnik liczb $(n - m, m)$.

Zapiszmy więc na mocy założenia indukcyjnego, że istnieją takie $k', l' \in \mathbb{Z}$, że $k'(n - m) + l'm = d$. Wtedy jednak $k'n + (l' - k')m = d$, więc przyjmując $k = k'$, $l = l' - k'$ uzyskujemy, że teza jest prawdziwa także dla pary (n, m). □

Lemat 2 (Euklides)**.** *Jeśli* p *jest liczbą pierwszą, zaś* $a, b \in \mathbb{Z}$*, to z tego, że* $p \mid ab$ *wynika, że* $p \mid a$ *lub* $p \mid b$.

Dowód. Załóżmy, że $p \mid ab$, zaś $p \nmid a$. Wtedy największy wspólny dzielnik liczb p, a musi wynosić jeden. Na mocy lematu 1 istnieją liczby $k, l \in \mathbb{Z}$, że $pk + la = 1$. Stąd $pkb + lab = b$. Jednakże $p \mid pkb$, $p \mid lab$, skąd wtedy $p \mid b$. □

Twierdzenie 1 (Jednoznaczność rozkładu na czynniki pierwsze)**.** *Każdą liczbę całkowitą dodatnią można jednoznacznie z dokładnością do permutacji zapisać jako iloczyn liczb pierwszych.*

Dowód. Najpierw udowodnimy indukcyjnie, że każdą liczbę całk. dod. da się zapisać na przynajmniej jeden sposób. Liczbę jeden można przestawić jako iloczyn pusty.

Załóżmy więc, że każdą liczbę całk. dod. mniejszą niż pewne $S > 1$ można zapisać jako iloczyn liczb pierwszych. Rozpatrzmy teraz liczbę S. Jest ona albo pierwsza, albo złożona. W każdym przypadku posiada jakiś dzielnik pierwszy p. Wtedy zauważmy, że z założenia indukcyjnego liczbę $\frac{S}{p}$ można zapisać jako iloczyn liczb pierwszych. Jednak dopisując do tego rozkładu liczbę p uzyskujemy rozkład liczby S.

Udowodnimy teraz, że taki rozkład jest jednoznaczny. Załóżmy bowiem nie wprost, że istnieje choć jedna liczba naturalna o niejednoznacznym rozkładzie na czynniki pierwsze. Na mocy zasady minimum istnieje najmniejsza taka liczba, oznaczmy ją n.

Gdyby $n = 1$, to mielibyśmy, że iloczyn niezerowej liczby liczb pierwszych jest równy jeden, co jest sprzecznością.

Załóżmy więc, że $1 < n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = q_1^{b_1} q_2^{b_2} \cdots q_l^{b_l}$, gdzie p_i, q_j są liczbami pierwszymi, zaś a_i, b_j liczbami całkowitymi dodatnimi dla $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant l$. Oczywiście $k, l > 0$.

Zauważmy jednak, że żadna z liczb q_j nie może być równa liczbie p_1, gdyż w przeciwnym wypadku także liczba $\frac{n}{p_1} < n$ posiadałaby niejednoznaczny rozkład na czynniki pierwsze powstały ze skreślenia liczby p_1 z dwóch rozkładów liczby n.

Niech r oznacza najmniejszą liczbę całkowitą dodatnią taką, że $p_1 \mid q_1^{b_1} q_2^{b_2} \cdots q_r^{b_r}$. Taka liczba istnieje, gdyż w szczególności $r = l$ spełnia zapisany przed chwilą warunek podzielności. Oczywiście $r > 1$, gdyż $p_1 \mid q_1^{b_1}$ oznaczałoby, że $q_1 = p_1$.

Jednak zauważmy, że na mocy lematu 2 mamy, że $p_1 \mid \left(q_1^{b_1} \cdots q_{r-1}^{b_{r-1}}\right) q_r^{b_r}$ implikuje, że $p_1 \mid q_r^{b_r}$ lub $p_1 \mid \left(q_1^{b_1} \cdots q_{r-1}^{b_{r-1}}\right)$. Pierwszy przypadek jest sprzecznością, gdyż wtedy $p_1 = q_r$, zaś drugi jest sprzecznością z minimalnością r.

Stąd rozkład liczby n musi być jednoznaczny, co dowodzi, że rozkład każdej liczby całk. dod. jest jednoznaczny. □

Powiemy, że $P(x) \in \mathbb{Z}[x]$ jest ładny, jeśli największy wspólny dzielnik jego współczynników jest równy 1.

Lemat 3 (Gauss)**.** *Jeśli* $P(x), Q(x) \in \mathbb{Z}[x]$ *są ładne, to* $P(x)Q(x)$ *też.*

Dowód. Zapiszmy $P(x) = p_0 + \ldots + p_n x^n$, $Q(x) = q_0 + \ldots + q_m x^m$, $P(x)Q(x) = r_0 + \ldots + r_{n+m} x^{n+m}$. Przypuśćmy, że jednak $P(x)Q(x)$ nie jest ładny. Wtedy istnieje liczba pierwsza p, że $p | r_0, r_1, \ldots, r_{n+m}$. Niech k, l będą najmniejszymi indeksami takimi, że $p \nmid p_k, q_l$. Popatrzmy na $r_{k+l} = \sum_{w=0}^{k+l} p_w q_{k+l-w}$, gdzie w razie