Jednoznaczność rozkładu w $\mathbb{N}$ – część 1

Bartłomiej BZDĘGA

Przed przystąpieniem do lektury zalecam zapoznanie się z kącikiem nr 23 (*Wykładniki p-adyczne*, Δ^{11}_{20}) oraz nr 29 (*Algorytm Euklidesa*, Δ^{5}_{21}).

Rozkładem liczby naturalnej $n > 1$ na czynniki pierwsze będziemy nazywali zapis

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}, \tag{1}$$

w którym $p_1, p_2, \ldots, p_k$ są różnymi liczbami pierwszymi oraz liczby $\alpha_1, \alpha_2, \ldots, \alpha_k$ są całkowite dodatnie.

Twierdzenie o jednoznaczności rozkładu mówi, że każda liczba naturalna $n > 1$ ma dokładnie jeden taki rozkład z dokładnością do kolejności czynników.

Dowód istnienia rozkładu. Najpierw zauważmy, że każda liczba naturalna $n > 1$ ma dzielnik pierwszy – wystarczy wziąć najmniejszy dzielnik n różny od 1 (gdyby nie był on liczbą pierwszą, to pewien jego dzielnik byłby jeszcze mniejszym dzielnikiem n różnym od 1).
Niech q_1 będzie dzielnikiem pierwszym liczby n. Są dwie możliwości: albo $n/q_1 = 1$, albo $n/q_1 > 1$ ma dzielnik pierwszy q_2. W drugim przypadku znów albo $n/(q_1q_2) = 1$, albo $n/(q_1q_2) > 1$ ma dzielnik pierwszy q_3 i tak dalej. W końcu dojdziemy do równości $n/(q_1q_2 \ldots q_t) = 1$, więc $n = q_1q_2 \ldots q_t$ i wystarczy ewentualnie pogrupować czynniki i zamienić iloczyny na potęgi, by otrzymać rozkład taki jak w (1).

Do wykazania jedyności rozkładu będziemy potrzebować następującego lematu.

Lemat Euklidesa. Niech p będzie dowolną liczbą pierwszą. Dla liczb naturalnych a i b zachodzi implikacja

$$p \mid ab \quad \Rightarrow \quad p \mid a \vee p \mid b. \tag{2}$$

Błędem jest dowodzenie implikacji (2) z użyciem twierdzenia o jednoznaczności rozkładu, ponieważ to jej potrzebujemy, aby udowodnić to twierdzenie. Kluczowe są tu wnioski z algorytmu Euklidesa, o których pisałem w kąciku nr 29.

Dowód lematu. Są dwie możliwości: $\mathtt{NWD}(a, p) = p$ lub $\mathtt{NWD}(a, p) = 1$. W pierwszym przypadku $p \mid a$, w drugim $p \mid b$ na mocy własności (1) z kącika nr 29. (Można, a nawet należy uogólnić: jeśli p jest liczbą pierwszą dzielącą iloczyn t liczb naturalnych, to p dzieli co najmniej jeden czynnik. Dowód przez indukcję względem t pozostawiam Czytelnikowi.)

Dowód jedyności rozkładu. Niech n będzie liczbą spełniającą równość (1) i $P = \{p_1, \ldots, p_k\}$. Jeśli $p \in P$, to oczywiście $p \mid n$. W drugą stronę, jeśli liczba pierwsza $p \mid n = p_1^{\alpha_1}p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, to p dzieli co najmniej jeden z czynników, co prowadzi do wniosku, że $p \in P$. Wobec tego zbiór P jest jednoznacznie wyznaczony – jest to zbiór wszystkich dzielników pierwszych liczby p.
Jest oczywiste, że $p_1^{\alpha_1} \mid n$. Ponadto $p_1^{\alpha} \nmid n$ dla $\alpha > \alpha_1$, gdyż w przeciwnym razie musiałaby zajść podzielność $p_1 \mid p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, co jest niemożliwe, bo p_1 nie dzieli żadnego z czynników. Z tego wynika, że $\alpha_1 = \nu_{p_1}(n)$, analogicznie $\alpha_i = \nu_{p_i}(n)$ dla $i = 1, 2, \ldots, k$. To dowodzi jednoznaczności wykładników.

Jednym z najprostszych zastosowań twierdzenia o jednoznaczności rozkładu w $\mathbb{N}$ jest rozwiązywanie równań diofantycznych – czyli takich, których niewiadome są liczbami całkowitymi. Równanie sprowadzamy do postaci $AB = n$, w której znamy rozkład liczby n na czynniki pierwsze i na jego podstawie potrafimy powiedzieć coś na temat A i B.

Zadania

1. Rozwiązać równanie $\sqrt{6xy + 2x - 3y} = 19$ w liczbach całkowitych x i y.
2. Rozwiązać równanie $m^2 = 2^n + 1$ w liczbach całkowitych dodatnich m, n.
3. Rozstrzygnąć, czy suma kilku (więcej niż jednej) kolejnych liczb całkowitych dodatnich może być potęgą dwójki o wykładniku naturalnym.
4. Wyznaczyć wszystkie pary liczb pierwszych (p, q), dla których $p \leqslant q$ oraz $p^2 + pq + q^2$ jest kwadratem liczby naturalnej.
5. Udowodnić, że równanie $(3x + 4y)(4x + 5y) = 7^z$ nie ma rozwiązań w liczbach całkowitych dodatnich x, y, z.
6. Wyznaczyć wszystkie trójki (x, y, n) liczb całkowitych dodatnich, spełniających równość $2x^2 + 5xy + 2y^2 = 3^n$.

Wskazówki do zadań

1. Równanie sprowadza się do postaci $(2x - 1)(3y + 1) = 360$. Liczbę przypadków można nieco ograniczyć: $2 \nmid 2x - 1$, więc $8 \mid 3y + 1$, analogicznie można wykazać, że $9 \mid 2x - 1$. Należy pamiętać, że liczby $2x - 1$ i $3y + 1$ muszą być nieparzyste.
2. Mamy $2^n = (m - 1)(m + 1)$. Jeśli iloczyn dwóch liczb jest potęgą liczby pierwszej, to każdy z czynników jest potęgą tej liczby. Stąd $m - 1$ i $m + 1$ to potęgi dwójki, które się różnią o 2.
3. Polowa sukcesu to zapisanie równania: $2^n = a + (a + 1) + \ldots + (a + k)$. Prawą stronę można zapisać jako iloczyn dwóch czynników, z których co najmniej jeden jest nieparzysty i większy od 1.
4. Rozwiązujemy równanie $p^2 + pq + q^2 = n^2$. Liczbę pq można tu zapisać jako różnicę kwadratów – obustronne dodanie pq na pewno w tym pomoże.
5. Ile razy liczba $4x + 5y$ może być większa niż $3x + 4y$, jeśli obie są potęgami siódemki?
6. Lewą stronę można zapisać w postaci iloczynu liczb całkowitych – oba czynniki muszą być potęgami trójki, powiedzmy 3^a i 3^b, przy czym $a, b \geqslant 0$ i $a + b = n$. Można dalej wyznaczyć x i y za pomocą a i b. Trzeba jeszcze sprawdzić, kiedy otrzymane wartości są całkowite dodatnie.