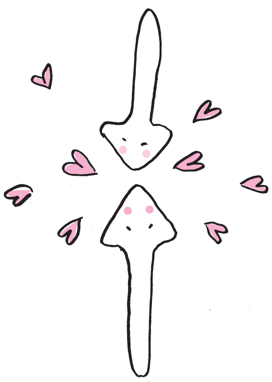
Jednoznaczność rozkładu w $\mathbb{N}$ – część 2

Bartłomiej BZDĘGA

Niech $n > 1$ będzie liczbą naturalną oraz niech
$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$
będzie rozkładem na czynniki pierwsze zgodnie z definicją z poprzedniego kącika. Pokażę tu kilka dalszych wniosków z twierdzenia o jednoznaczności rozkładu w $\mathbb{N}$.

Jeśli $n = a^2$ dla pewnej liczby naturalnej a, to wykładniki w rozkładzie liczby n na czynniki pierwsze są podwojonymi wykładnikami z rozkładu liczby a, wszystkie są zatem parzyste. W drugą stronę, jeśli $\alpha_1, \alpha_2, \ldots, \alpha_k$ są parzyste, to $\sqrt{n} = p_1^{\alpha_1/2} p_2^{\alpha_2/2} \ldots p_k^{\alpha_k/2}$ jest liczbą naturalną. Wnioskujemy zatem, że liczba n jest kwadratem liczby naturalnej wtedy i tylko wtedy, gdy wszystkie wykładniki w jej rozkładzie na czynniki pierwsze są parzyste. Ogólniej – liczba n jest t-tą potęgą liczby naturalnej wtedy i tylko wtedy, gdy wszystkie wykładniki w jej rozkładzie na czynniki pierwsze dzielą się przez t; dowód jest zasadniczo taki sam.



Rozkład na czynniki pierwsze daje też nieco inne (bardziej szkolne niż algorytm Euklidesa) spojrzenie na liczby względnie pierwsze. Jeżeli $\mathtt{NWD}(m,n) > 1$, to liczba $\mathtt{NWD}(m,n)$ ma dzielnik pierwszy, który jest wspólnym dzielnikiem m i n, więc występuje w ich rozkładach na czynniki pierwsze. Implikacja odwrotna zachodzi w oczywisty sposób. Możemy stąd wywnioskować, że $\mathtt{NWD}(m,n) = 1$ wtedy i tylko wtedy, gdy każda liczba pierwsza z rozkładu liczby n jest inna niż wszystkie liczby pierwsze z rozkładu m.

Łącząc powyższe dwie równoważności, możemy na przykład udowodnić, że jeśli iloczyn liczb względnie pierwszych m i n jest kwadratem liczby naturalnej, to obie te liczby również są kwadratami liczb naturalnych – ten fakt przyda się w zadaniach 1 i 2. Zapiszmy $m \cdot n = q_1^{\beta_1} q_2^{\beta_2} \ldots q_l^{\beta_l} \cdot p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ – jest to rozkład na czynniki pierwsze, ponieważ wszystkie p_i i q_j są różne. Liczba mn jest kwadratem, więc wszystkie α_i i β_j są parzyste i w konsekwencji m i n są kwadratami liczb naturalnych. Analogiczne twierdzenia zachodzą oczywiście również dla wyższych wykładników.

Na koniec, rozkład na czynniki pierwsze pozwala na dokonanie pewnych specyficznych podstawień. Opiszę tu jedno. Podstawmy $\alpha_i = 2a_i + w_i$, przy czym a_i jest liczbą całkowitą nieujemną oraz $w_i \in \{0,1\}$ (jest to po prostu zapis dzielenia przez 2 z resztą). Otrzymamy $n = k^2 b$ dla $k = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ oraz $b = p_1^{w_1} p_2^{w_2} \ldots p_k^{w_k}$. Liczba b jest iloczynem kilku różnych liczb pierwszych. Takie liczby, zwane bezkwadratowymi (bo nie są podzielne przez kwadrat żadnej liczby pierwszej), mają ciekawą własność wzmacniania podzielności, która jest pomocna w zadaniach 3 i 4.
Niech b będzie liczbą bezkwadratową i $b \mid m^t$, dla pewnych liczb całkowitych dodatnich m i t. Każdy dzielnik pierwszy liczby b jest dzielnikiem m^t, więc występuje w rozkładzie liczby m na czynniki pierwsze. Z tego wynika, że $b \mid m$.

Zadania

1. Dana jest liczba całkowita dodatnia n i liczba pierwsza p, dla których $n^2 + np$ jest kwadratem liczby naturalnej. Wykazać, że n również jest kwadratem liczby naturalnej.
2. Liczby całkowite dodatnie a, b, c są parami względnie pierwsze i spełniają równość $a^2 + b^2 = c^2$, ponadto b jest liczbą parzystą. Udowodnić, że istnieją takie liczby naturalne m i n, że $a = m^2 - n^2$, $b = 2mn$ i $c = m^2 + n^2$.
3. Różne liczby całkowite dodatnie m i n spełniają podzielność $m \mid n^2$. Udowodnić, że $|m - n| \geqslant \sqrt{m}$.
4. Liczby całkowite dodatnie m i n spełniają podzielność $mn \mid m^2 + n^2 + m$. Wykazać, że m jest kwadratem liczby całkowitej.
5. Liczbę naturalną n nazwiemy *dobrą*, jeśli istnieje taka liczba pierwsza p, że $p \mid n$, ale $p^2 \nmid n$. Dowieść, że wśród liczb $1, 2, 3, \ldots, 10^{12}$ liczby dobre stanowią co najmniej 99%.

Wskazówki do zadań

1. Z algorytmu Euklidesa otrzymamy $\mathtt{NWD}(n, n+p) \in \{1, p\}$. Jeśli $n = kp$ dla pewnego naturalnego k, to $n^2 + np$ nie jest kwadratem liczby naturalnej (dlaczego?). Stąd $p \nmid n$, więc $\mathtt{NWD}(n, n+p) = 1$.

2. Liczby a i c są nieparzyste. Równość przekształcić do postaci $(b/2)^2 = \frac{c-a}{2} \cdot \frac{c+a}{2}$ i wykazać, że $\mathtt{NWD}\left(\frac{c-a}{2}, \frac{c+a}{2}\right) = 1$.

3. Niech $m = k^2 b$ dla liczby naturalnej k i liczby bezkwadratowej b. Uzasadnić, że $kb \mid n$, i wywnioskować, że $|m - n| \geqslant kb \geqslant \sqrt{m}$.

4. Podstawmy $m = k^2 b$ dla liczby naturalnej k i liczby bezkwadratowej b. Wywnioskować, że $kb \mid n$, i podstawić $n = kbl$. Z danej podzielności otrzymać wniosek, że $b \mid 1$, czyli $b = 1$.

5. Uzasadnić, że każdą liczbę ze zbioru $\{1, 2, \ldots, 10^{12}\}$, która nie jest dobra, można zapisać (niekoniecznie jednoznacznie) w postaci $a^2 b^3$, dla pewnych liczb całkowitych dodatnich $a \leqslant 10^6$ i $b \leqslant 10^4$.