

Niech  $P$  będzie polem figury ograniczonej przez krzywą  $\mathcal{C}$ . Stosując wzór (3) do parametryzacji krzywych  $\mathcal{C}$  i  $\mathcal{O}$ , otrzymujemy:

$$P = \int_0^L x_c(t)y_c'(t) dt = \int_0^L x_o(t)y_c'(t) dt,$$

$$\pi r^2 = - \int_0^L y_o(t)x_o'(t) dt = - \int_0^L y_o(t)x_c'(t) dt.$$

Dodajmy powyższe równości stronami:

$$(4) \quad P + \pi r^2 = \int_0^L (x_o(t)y_c'(t) - y_o(t)x_c'(t)) dt.$$

Funkcja podcałkowa jest iloczynem skalarnym wektora  $v_o^*(t) = (-y_o(t), x_o(t))$  i wektora prędkości  $v_c(t)$ . Mamy  $|v_o^*(t)| = r$ , gdyż  $(x_o(t), y_o(t)) \in \mathcal{O}$  oraz  $|v_c(t)| = 1$ . Iloczyn skalarny dwóch wektorów nie przekracza iloczynu ich długości, więc

$$P + \pi r^2 \leq \int_0^L r dt = Lr.$$

Teraz wystarczy zastosować nierówność między średnią arytmetyczną i geometryczną:

$$(5) \quad \sqrt{P \cdot \pi r^2} \leq \frac{P + \pi r^2}{2} \leq \frac{Lr}{2}.$$

Nierówność  $\sqrt{P \cdot \pi r^2} \leq \frac{Lr}{2}$  trzeba podzielić obustronnie przez  $\frac{r}{2}$  i podnieść do kwadratu, by otrzymać nierówność (1).

## Równość tylko dla koła

Pozostaje wykazać, że jeśli  $L^2 = 4\pi P$ , to krzywa  $\mathcal{C}$  jest okręgiem. W tym celu prześledzimy te miejsca dowodu nierówności (1), w których szacowaliśmy – w każdej z nierówności w (5) musi być równość.

W pierwszej nierówności równość zachodzi tylko, gdy  $P = \pi r^2$ , i wówczas  $L = \sqrt{4\pi P} = \sqrt{4\pi^2 r^2} = 2\pi r$ . W drugiej korzystaliśmy z szacowania iloczynu skalarnego niezerowych wektorów. Jest równy iloczynowi ich długości tylko, gdy kąt między nimi jest zerowy – czyli jeden z wektorów jest równy drugiemu pomnożonemu przez pewną liczbę dodatnią. Biorąc pod uwagę długości tych wektorów, mamy  $v_o^*(t) = r v_c(t)$ , czyli w szczególności

$$(6) \quad x_c(t) = x_o(t) = r y_c'(t).$$

Nierówności (1) można dowieść alternatywnie, rozważając okrąg  $\Omega$  o środku w punkcie  $(0, 0)$  i promieniu  $s$  oraz taką parametryzację dodatnią  $\Omega(t)$ , że odcinek  $\mathcal{C}(t)\Omega(t)$  jest dla każdego  $t$  równoległy do osi  $OX$ . Analizując miejsca szacowania w tym alternatywnym dowodzie (wszystko przebiega tak samo, jak to zostało opisane w akapicie wyżej), dochodzimy do wniosku, że  $P = \pi s^2$ , więc  $s = r$ . Z równości w szacowaniu iloczynu skalarnego otrzymamy

$$(7) \quad y_c(t) = s \dot{x}_c(t) = r \dot{x}_c(t).$$

Równości (6) i (7) dają

$$\sqrt{x_c(t)^2 + y_c(t)^2} = r \sqrt{y_c'(t)^2 + \dot{x}_c(t)^2} = r |v_c(t)| = r,$$

więc  $\mathcal{C}$  jest okręgiem o środku  $(0, 0)$  i promieniu  $r$ .

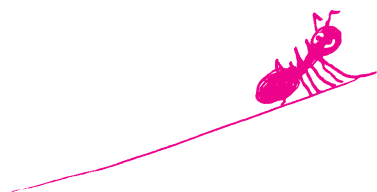
## O pewnych hipotezach teorii liczb

Witold BEDNAREK\*

Rozpocznijmy od następującego zadania: udowodnić, że dla dowolnej liczby naturalnej  $m$  liczba  $m^2 + 3m + 2$  jest złożona. Nie jest to wymagający problem; rozwiązanie polega na zauważeniu, że badaną liczbę można przedstawić jako  $(m + 1)(m + 2)$  i oba czynniki są zawsze liczbami całkowitymi, większymi niż 1. A co, jeśli zamiast tego spytamy o liczby postaci  $m^2 + m + 2$ ? Tutaj poprzednia sztuczka już nie zadziała; wielomianu  $w(x) = x^2 + x + 2$  nie jesteśmy w stanie przedstawić jako iloczynu dwóch wielomianów o współczynnikach całkowitych, różnych od wielomianu tożsamościowo równego 1. Takie wielomiany (o współczynnikach całkowitych) nazywamy *niezrozkładalnymi*. Jeśli jednak przyjrzymy się wartościom  $w(m)$  dla  $m = 1, 2, \dots$ , zaobserwujemy, że wszystkie są parzyste i większe od 2, zatem złożone. Nietrudno uzasadnić, dlaczego tak jest dla dowolnej liczby naturalnej  $m$ : nierówność  $w(m) > 2$  jest oczywista, a parzystość  $w(m)$  wynika z faktu, że  $w(m) = m(m + 1) + 2$  i któraś z liczb  $m$  lub  $m + 1$  jest parzysta.

Czy teza naszego zadania może być prawdziwa, jeśli żaden z przedstawionych dwóch argumentów nie ma zastosowania? W 1857 roku Wiktor Buniakowski sformułował hipotezę, że nie. Niech  $f$  będzie wielomianem niezrozkładalnym o współczynnikach całkowitych i dodatnim współczynnikiem przy najwyższej potędze. Ponadto niech wielomian  $f$  ma stopień co najmniej 2 oraz nie istnieje taka liczba naturalna  $n > 1$ , która dzieli wartości  $f(k)$  dla każdego naturalnego  $k$ . Wtedy, wedle hipotezy Buniakowskiego, istnieje nieskończenie wiele takich liczb naturalnych  $m$ , że liczba  $f(m)$  jest pierwsza.

\* Nauczyciel, I Liceum im. Mikołaja Kopernika w Łodzi



**Przykład 1.** Niech  $f(x) = x^2 + 1$ . Wielomian ten spełnia założenia hipotezy Buniakowskiego, z której wynikałoby, że istnieje nieskończenie wiele liczb pierwszych postaci  $m^2 + 1$ . Na przykład liczby:

$$\begin{array}{lll} 1^2 + 1 = 2, & 4^2 + 1 = 17, & 10^2 + 1 = 101 \\ 2^2 + 1 = 5, & 6^2 + 1 = 37, & \end{array}$$

są liczbami pierwszymi.

W 1978 roku Henryk Iwaniec (uczeń Andrzeja Schinzla) udowodnił coś bliskiego hipotezie Buniakowskiego w przypadku z przykładu 1: uzasadnił, że istnieje nieskończenie wiele takich liczb naturalnych  $m$ , dla których liczba  $m^2 + 1$  jest liczbą pierwszą lub iloczynem dwóch liczb pierwszych.

**Przykład 2.** Niech  $f(x) = x^2 + x + 41$ . Wielomian ten spełnia założenia hipotezy Buniakowskiego, z której wynikałoby, że istnieje nieskończenie wiele liczb pierwszych postaci  $m^2 + m + 41$ . Wspomnijmy, że wielomian ten był rozważany przez Leonharda Eulera, który zauważył, że liczby  $f(0), f(1), \dots, f(39)$  są pierwsze.

Jak już wcześniej zauważyliśmy, dla dowolnej liczby naturalnej  $m$  któraś z liczb  $m$  oraz  $m + 1$  jest parzysta (więc, poza  $m = 1, 2$ , złożona). Nie ma jednak widocznego powodu, dla którego nie mogłoby istnieć nieskończenie wiele par liczb pierwszych postaci  $m$  i  $m + 2$ . Takie liczby pierwsze nazywamy *bliźniaczymi*, przykładami są:

$$\begin{array}{lll} 3 \text{ i } 5, & 11 \text{ i } 13, & 29 \text{ i } 31, \\ 5 \text{ i } 7, & 17 \text{ i } 19, & 41 \text{ i } 43; \end{array}$$

hipoteza liczb bliźniaczych stwierdza, że takich par jest nieskończenie wiele. W 1904 roku Leonard E. Dickson sformułował istotne uogólnienie tej hipotezy: Niech  $s \geq 1$  będzie dowolnie ustaloną liczbą naturalną oraz  $f_i(x) = a_i x + b_i$  dla  $i = 1, \dots, s$ , gdzie liczby  $a_1, \dots, a_s > 0$  oraz  $b_1, \dots, b_s$  są całkowite. Załóżmy ponadto, że nie istnieje taka liczba pierwsza  $p > 1$ , która dzieli iloczyn  $f_1(k) \cdot \dots \cdot f_s(k)$  dla każdego naturalnego  $k$ . Wtedy istnieje nieskończenie wiele takich liczb naturalnych  $m$ , że każda z liczb  $f_1(m), \dots, f_s(m)$  jest pierwsza.

**Przykład 3.**  $s = 2$ ,  $f_1(x) = x$ ,  $f_2(x) = x + 2$ . Wówczas dostajemy hipotezę o liczbach bliźniaczych.

**Przykład 4.**  $s = 2$ ,  $f_1(x) = x$ ,  $f_2(x) = 2x + 1$ . W tym przypadku prawdziwość hipotezy Dicksona oznaczałoby, że istnieje nieskończenie wiele liczb pierwszych postaci  $2m + 1$ , gdzie  $m$  jest liczbą pierwszą. Takie liczby nazywamy liczbami Sophie Germain, przykładami są:

$$\begin{array}{ll} 5 = 2 \cdot 2 + 1, & 11 = 2 \cdot 5 + 1, \\ 7 = 2 \cdot 3 + 1, & 23 = 2 \cdot 11 + 1. \end{array}$$

Skoro mamy liczby pierwsze bliźniacze, to nasuwa się pytanie o liczby pierwsze *trojacze*. W pierwszym odruchu można by pomyśleć, że są to trójki liczb pierwszych postaci  $m$ ,  $m + 2$  i  $m + 4$ . Poza przypadkiem  $m = 3$  takich trójek jednak nie ma, co można wywnioskować z faktu, że liczby  $m$ ,  $m + 2$  i  $m + 4$  dają różne reszty z dzielenia przez 3. Może w takim

razie poszukać trójek liczb pierwszych postaci  $m$ ,  $m + 3$  i  $m + 6$ ? To też zły pomysł, ze względu na różną parzystość liczb  $m$  i  $m + 3$ . Po chwili namysłu dochodzimy do wniosku, że najbliższej idei *pierwszych trojaczków* byłyby trójki  $m$ ,  $m + 2$  i  $m + 6$ , na przykład:

$$\begin{array}{lll} (5, 7, 11), & (17, 19, 23), & \\ (11, 13, 17), & (41, 43, 47), & (101, 103, 107), \end{array}$$

lub  $m$ ,  $m + 4$  i  $m + 6$ , na przykład:

$$\begin{array}{lll} (7, 11, 13), & (37, 41, 43), & (97, 101, 103). \\ (13, 17, 19), & (67, 71, 73), & \end{array}$$

Hipoteza Dicksona pociągałaby za sobą istnienie nieskończenie wielu trojaczków obu typów.

Rozważmy teraz dowolną liczbę naturalną  $r > 0$ . Zastanówmy się, jak długi może być ciąg arytmetyczny o różnicy  $r$ , złożony z samych liczb pierwszych. Przypadek  $r = 2$  już rozważyliśmy – trójka  $(3, 5, 7)$  to jedyny ciąg arytmetyczny liczb pierwszych o różnicy 2 i długości 3 (w szczególności, nie ma dłuższego takiego ciągu). Załóżmy zatem, że  $r \geq 3$ . Niech  $p_1, p_2, \dots, p_n$  będzie najdłuższym takim ciągiem i niech  $q$  będzie najmniejszą liczbą pierwszą, która nie dzieli  $r$ . Przypuśćmy, że  $n \geq q$ . Ponieważ  $q$  jest liczbą pierwszą i  $q \nmid r$ , to liczby  $p_1, \dots, p_q$  dają różne reszty z dzielenia przez  $q$ ; skoro liczb tych jest co najmniej  $q$ , występuje wśród nich liczba  $p_i$  podzielna przez  $q$ , a że są to liczby pierwsze, musi być  $p_i = q$ . Ponadto różnica między kolejnymi dwoma jest równa  $r$  (czyli, dla  $r \geq 3$ , więcej niż  $q$ ), a zatem  $i = 1$ . Wynika stąd również, że w takim wypadku  $n = q$  (gdyby  $n > q$ , to  $p_{q+1} = q(1 + r)$  byłoby liczbą złożoną). Z drugiej strony, z prawdziwości hipotezy Dicksona wynikałoby, że istnieje nieskończenie wiele ciągów arytmetycznych liczb pierwszych o różnicy  $r$  długości  $q - 1$ .

**Przykład 5.** Weźmy  $r = 6$ . Mamy tu  $q = 5$ , zatem  $n \leq 5$ . Jeśli  $n = 5$ , musi być  $p_1 = 5$ . Sprawdzamy, że ciąg arytmetyczny  $(5, 11, 17, 23, 29)$  o różnicy 6 składa się z samych liczb pierwszych. Niech teraz  $r = 36$ . Ponownie  $q = 5$ , więc sprawdzamy ciąg  $(5, 41, 77, 113, 149)$ , ale liczba 77 jest złożona. Wobec tego musi być  $n < 5$ . Zgodnie z hipotezą Dicksona czterowrazowych ciągów arytmetycznych liczb pierwszych o różnicy  $r = 36$  jest nieskończenie wiele. Takim jest na przykład ciąg  $(31, 67, 103, 139)$ .

Artykuł zakończymy przedstawieniem *hipotezy Schinzla*, która jest uogólnieniem jednocześnie hipotezy Buniakowskiego i hipotezy Dicksona. Hipoteza Schinzla orzeka, że hipoteza Dicksona jest prawdziwa również, gdy zamiast funkcji liniowych weźmiemy dowolne wielomiany nierozkładalne (przy założeniu o braku „trywialnych podzielności”, wynikających z prostych kongruencji, podobnie jak w hipotezie Buniakowskiego).

**Przykład 6.**  $s = 2$ ,  $f_1(x) = x$ ,  $f_2(x) = x^2 + x + 1$ .

Na przykład liczby

$$\begin{array}{ll} 2^2 + 2 + 1 = 7, & 5^2 + 5 + 1 = 31, \\ 3^3 + 3 + 1 = 13, & 17^2 + 17 + 1 = 307 \end{array}$$

są liczbami pierwszymi.