Jest to zapis odczytu wygłoszonego na XLII Szkole Matematyki Poglądowej, *Dowody i kontrprzykłady*, styczeń 2009.

# O pewnym kontrprzykładzie

*Maciej ULAS, Kraków*

Matematyk jest jak podróżnik, którego celem jest odkrywanie nowych lądów. Nowe lądy w matematyce nazywamy twierdzeniami. Jednak, żeby matematyczne odkrycie zostało powszechnie uznane, i nosiło dumne miano *twierdzenie*, musi posiadać dowód. Dowód jest zatem jak podróż, którą musi odbyć odkrywca nowych lądów. Jak wiadomo, podróże w nieznane bywają niebezpieczne i pełne pułapek. Na szczęście, matematyk nie jest narażony na bezpośrednie fizyczne niebezpieczeństwo, gdyż podczas przeprowadzania dowodu jakiegoś twierdzenia podróżuje on jedynie pośród swych myśli (dodajmy jeszcze, że wraz z jego myślami podróżuje ręka uzbrojona w ołówek lub długopis). W momencie, gdy dowód twierdzenia jest już gotowy (czasem trwa to bardzo długo), matematyk pisze pracę i wysyła ją do jednego z czasopism matematycznych. Praca jest recenzowana przez innego matematyka (lub matematyków), a następnie, gdy spełnia wszystkie wymagania, a w szczególności nie zawiera błędów, zostaje opublikowana. W tym miejscu podróż matematyka się kończy, lecz teraz rozpoczyna się nasza podróż drogi Czytelniku. Podróż, która ma nas przekonać, że nie wszystkie publikowane twierdzenia ... są prawdziwe i nie warto wierzyć bezkrytycznie we wszystko, co się czyta. Będzie to podróż, w której poznamy (a w zasadzie przypomnimy) dwie wielkie hipotezy teorii liczb, skonstruujemy krzywą wymierną na pewnej powierzchni i obalimy jedno „twierdzenie" (zdanie, które nie jest udowodnione lub jego dowód jest niepoprawny nie może być twierdzeniem – może być co najwyżej „twierdzeniem").

By być bardziej precyzyjnym wyjawmy cel naszej podróży: celem naszej podróży będzie pokazanie, że poniższe „twierdzenie" nie jest twierdzeniem.

**Twierdzenie 0.1 (Tw. 8 (ii) z [3]).** *Załóżmy, że hipotezy* abc *i* abcd *są prawdziwe. Niech* $f \in \mathbb{Z}[x]$, $\deg f = n$ *i załóżmy, że* $f$ *nie ma pierwiastków wielokrotnych. Jeśli istnieje wielomian* $h \in \mathbb{Z}[x]$ *względnie pierwszy z* $f$ *i taki, że* $h(x)(f(x) - h(x))$ *ma mniej niż* $n/10$ *różnych pierwiastków, to istnieje tylko skończenie wiele liczb bezkwadratowych* $d$ *o tej własności, że istnieje więcej niż jedno wymierne rozwiązanie równania* $f(x) = dy^2$.

W sformułowaniu tego „twierdzenia" występuje kilka pojęć, które należy przypomnieć lub zdefiniować.

Zaczniemy od przypomnienia pojęcia liczby bezkwadratowej. Mówimy, że liczba całkowita $d$ jest *bezkwadratowa*, jeśli nie jest ona podzielna przez kwadrat żadnej liczb pierwszej.

O hipotezach abc i abcd można przeczytać w *Delcie* z 2000 roku [1, 2]. Nasze sformułowanie tych hipotez będzie różnić od tych przedstawionych w *Delcie* (są jednak z nimi równoważne). Zanim przypomnimy, co te hipotezy mówią, zdefiniujmy jeszcze funkcję $\mathrm{rad} : \mathbb{Z} \ni n \mapsto \mathrm{rad}(n) \in \mathbb{N}$ daną przez równość

$$\mathrm{rad}(n) = \prod_{p|n} p.$$

Innymi słowy: $\mathrm{rad}(n)$ jest iloczynem liczb pierwszych dzielących liczbę $n$. Liczba $\mathrm{rad}(n)$ bywa nazywana również *jądrem bezkwadratowym* liczby $n$.

**Hipoteza 0.2 (Hipoteza** abc**).** *Jeśli* $a, b, c \in \mathbb{Z}$ , $\mathrm{NWD}(a, b, c) = 1, a + b + c = 0$ *i żadna z podsum nie znika, to dla każdego* $\epsilon > 0$ *istnieje taka stała* $C(\epsilon)$*, że*

$$\max\{|a|, |b|, |c|\} < C(\epsilon)\,\mathrm{rad}(abc)^{1+\epsilon}.$$

Naturalnym uogólnieniem tej hipotezy jest następująca

**Hipoteza 0.3 (Hipoteza** abcd**).** *Jeśli* $a, b, c, d \in \mathbb{Z}$ ,
$\mathrm{NWD}(a, b, c, d) = 1, a + b + c + d = 0$ *oraz żadna z podsum nie znika, to dla każdego* $\epsilon > 0$ *istnieje taka stała* $C(\epsilon)$*, że*

$$\max\{|a|, |b|, |c|, |d|\} < C(\epsilon)\,\mathrm{rad}(abcd)^{3+\epsilon}.$$

Czytelnik zechce sprawdzić, wykorzystując równość
$2^{3k} + 3 \cdot 2^k(2^k + 1) + 1 - (2^k + 1)^3 = 0$, że wykładnik 3 w powyższej hipotezie jest konieczny.

Te dwie niewinnie wyglądające hipotezy mają bardzo dużo głębokich konsekwencji w teorii liczb i geometrii algebraicznej. W szczególności, Hipoteza abc implikuje prawdziwość hipotezy Mordella (obecnie Twierdzenie Faltingsa), która mówi, że zbiór punktów wymiernych na krzywych rodzaju $> 1$ jest skończony. Człowiek, który udowodni lub obali którąkolwiek z nich zdobędzie nieśmiertelność.

Przypomnijmy, że punkt $P = (x(P), y(P))$ leżący na krzywej $C:\ F(x, y) = 0$, gdzie $F \in \mathbb{Z}[x, y]$ nazywamy wymiernym, jeśli $x(P), y(P) \in \mathbb{Q}$. Zbiór punktów wymiernych na krzywej $C$ będziemy oznaczać przez $C(\mathbb{Q})$, dokładniej

$$C(\mathbb{Q}) = \{(x, y) \in \mathbb{Q} \times \mathbb{Q} :\ F(x, y) = 0\}.$$

Niech $f \in \mathbb{Z}[x]$ będzie wielomianem bez pierwiastków wielokrotnych i załóżmy, że $\deg f \geq 5$. Wówczas, krzywą postaci

$$\mathcal{C}:\ y^2 = f(x),$$

nazywamy *krzywą hipereliptyczną*. Jeśli dodatkowo $d \in \mathbb{Z}$ jest liczbą bezkwadratową, to krzywą $\mathcal{C}_d$ zadaną równaniem

$$\mathcal{C}_d:\ dy^2 = f(x),$$

nazywamy *skręceniem kwadratowym krzywej $\mathcal{C}$ przez $d$.*

Założenie, że $d$ jest liczbą całkowitą nie jest istotne, gdyż w przypadku $d = p/q \in \mathbb{Q} \setminus \mathbb{Z}$, gdzie $\mathrm{NWD}(p, q) = 1$, widzimy, że krzywe $\mathcal{C}_d$ i $\mathcal{C}_{q^2 d}$ są izomorficzne poprzez odwzorowanie $\varphi : \mathcal{C}_d \ni (x, y) \mapsto (x, y/q) \in \mathcal{C}_{q^2 d}$ i oczywiście $q^2 d \in \mathbb{Z}$. Ponadto, zauważmy, że jeśli $P = (x, y) \in \mathcal{C}(\mathbb{Q})$ i $y \neq 0$, to również punkt $Q = (x, -y)$ jest wymierny.

Krzywe $\mathcal{C}$ i $\mathcal{C}_d$ są określone nad ciałem liczb wymiernych. Nazwa krzywej $\mathcal{C}_d$ jest ściśle związana z zależnością łączącą krzywe $\mathcal{C}$ i $\mathcal{C}_d$. Mianowicie, jeśli do ciała $\mathbb{Q}$ dołączymy liczbę $\sqrt{d}$, czyli przejdziemy do rozszerzenia ciał $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ (jest to rozszerzenie algebraiczne stopnia 2), to krzywe $\mathcal{C}$ i $\mathcal{C}_d$ będą izomorficzne poprzez odwzorowanie

$$\Phi : \mathcal{C} \ni (x, y) \mapsto \left(x, \frac{y}{\sqrt{d}}\right) \in \mathcal{C}_d$$

z odwrotnością

$$\Phi^{-1} : \mathcal{C}_d \ni (x, y) \mapsto (x, \sqrt{d}y) \in \mathcal{C}.$$

Zdefiniowaliśmy wszystkie pojęcia występujące w Twierdzeniu 0.1. Teraz musimy się zastanowić w jaki sposób tego typu stwierdzenie można obalić? Wydaje się, że najlepszym pomysłem jest ... zacząć od końca. Dlaczego? Jest jasne, że by marzyć o skonstruowaniu kontrprzykładu musimy znaleźć taki wielomian $f \in \mathbb{Z}[x]$ wysokiego stopnia (co najmniej 10), że istnieje nieskończenie wiele bezkwadratowych liczb całkowitych $d$ o tej własności, że na krzywej $\mathcal{C}_d:\ dy^2 = f(x)$ leżą co najmniej dwa nietrywialne punkty wymierne $P_i = (x_i, y_i),\ i = 1, 2$. Tutaj słowo nietrywialny oznacza, że współrzędne punktów $P_i$ spełniają dwa warunki: $x_1 \neq x_2$ oraz $y_1 y_2 \neq 0$. Widzimy więc, że nasze zadanie sprowadza się do wskazania wielomianu $f \in \mathbb{Z}[x]$ o tej własności, że układ równań

$$dy_1^2 = f(x_1), \quad dy_2^2 = f(x_2), \tag{1}$$

ma nieskończenie wiele rozwiązań w liczbach wymiernych $x_1, y_1, x_2, y_2, d$. Łatwo zauważyć, że powyższy układ jest równoważny następującemu

$$d = \frac{f(x_1)}{y_1^2} = \frac{f(x_2)}{y_2^2}. \tag{2}$$

Zauważmy, że drugie równanie naszego układu można zapisać w postaci $y_2^2 f(x_1) = y_1^2 f(x_2)$. Bez straty dla ogólności możemy podstawić $y_1 = 1$. Teraz stoimy przed dylematem wyboru wielomianu $f$. Jak wybrać wielomian $f$ stopnia co najmniej 10, bez pierwiastków wielokrotnych i o tej własności, że na powierzchni $y_2^2 f(x_1) = f(x_2)$ leży punkt wymierny, dla którego $y_2 \neq 1$? Jest to

trudne pytanie. My jednak mamy szczęście, gdyż jak się przekonamy, wielomian $f(x) = x^n + ax + b$, gdzie $n$ jest dowolną liczbą naturalną i $a, b \in \mathbb{Z} \setminus \{0\}$, nadaje się doskonale do naszych celów. Dlaczego akurat ten wielomian, a nie inny? Cóż, odpowiedź z pewnością nie usatysfakcjonuje Czytelnika w pełni. Wielomian ten pojawił się w związku z badaniem problemu konstrukcji punktów wymiernych na krzywych hipereliptycznych nad ciałami skończonymi. Innymi słowy pojawia się on w zupełnie innym zagadnieniu, o którym więcej można przeczytać w pracy [5]. Dodajmy jeszcze, że jest to jeden z dwóch znanych wielomianów (drugim jest wielomian $f(x) = x^n + ax^2 + bx$), który posiada pożądane przez nas własności.

Widzimy zatem, że problem znalezienia nieskończenie wielu rozwiązań wymiernych układu (2) sprowadza się do wykazania, że zbiór punktów wymiernych na powierzchni $\mathcal{S}$ danej równaniem

$$\mathcal{S}: \; y_2^2 f(x_1) = f(x_2), \quad f(x) = x^n + ax + b,$$

jest nieskończony. Jeśli uda się nam to pokazać, to każde $d$ (wymierne) dane przez równość $d = f(x_1) = f(x_2)/y_2^2$ będzie spełniało żądane warunki.

**Twierdzenie 0.4.** *Zbiór punktów wymiernych na powierzchni $\mathcal{S}$ jest nieskończony.*

*Dowód.* Okazuje się, że można udowodnić coś więcej. Wykażemy mianowicie, że na powierzchni $\mathcal{S}$ leży krzywa wymierna. Innymi słowy, wykażemy, że istnieją niestałe funkcje wymierne $x_1(t), x_2(t), y_2(t)$, które spełniają równanie definiujące naszą powierzchnię $\mathcal{S}$. By tego dowieść wykorzystamy metodę współczynników nieoznaczonych. Zdefiniujmy $F(x_1, x_2, y_2) := y_2^2 f(x_1) - f(x_2)$. Niech $t$ i $T$ będą zmiennymi, a następnie połóżmy

$$x_1 = T, \quad x_2 = t^2 T, \quad y_2 = t^n.$$

Stąd otrzymujemy, że

$$F(T, t^2T, t^n) = t^{2n}(T^n + aT + b) - (t^{2n}T^n + at^2T + b) = a(t^{2n} - t^2)T + b(t^{2n} - 1).$$

Magia! Stopień wielomianu $F(T, t^2T, t^n)$ względem $T$ jest równy jeden. Możemy bez trudu rozwiązać równanie $F(T, t^2T, t^n) = 0$ względem $T$ i otrzymamy

$$T = T(t) = -\frac{b}{a}\frac{t^{2n} - 1}{t^{2n} - t^2}. \tag{3}$$

Wykorzystując znalezioną wartość $T$ możemy napisać równania naszej krzywej wymiernej, leżącej na powierzchni $\mathcal{S}$, w postaci

$$x_1(t) = -\frac{b}{a}\frac{t^{2n} - 1}{t^{2n} - t^2}, \quad x_2(t) = -\frac{b}{a}\frac{t^{2n} - 1}{t^{2(n-1)} - 1}, \quad y_2(t) = t^n.$$

Zwróćmy uwagę, że warunek $ab \neq 0$ jest istotny. □

**Uwaga 0.5.** Należy dodać, że jest to bardzo szczególny przypadek twierdzenia udowodnionego w pracy [5].

Wykorzystamy teraz otrzymany wynik do zdefiniowania nieskończonej rodziny liczby wymiernych $d$, która posłuży nam do obalenia Twierdzenia 0.1.

Zdefiniujmy $d(t) = f(T(t))$, gdzie funkcja wymierna $T$ jest dana przez (3) i $f(x) = x^n + ax + b$. Dla tak określonego $T$ rozważmy rodzinę krzywych $\{C_t\}_{t\in\mathbb{Q}}$ daną przez

$$C_t: \; d(t)y^2 = x^n + ax + b.$$

Wówczas z Twierdzenia 0.4 widzimy, że na krzywej $C_t$ mamy dwa punkty wymierne

$$P_1 = (T(t),\ 1), \quad P_2 = \left(-\frac{b}{a}\frac{t^{2n} - 1}{t^{2(n-1)} - 1},\ t^n\right).$$

Z naszego rozumowania wynika natychmiastowy

**Wniosek 0.6.** *Twierdzenie* 0.1 *jest nieprawdziwe.*

*Dowód.* Rozważmy skonstruowaną przez nas rodzinę krzywych $C_t$ i weźmy wielomian $h(x) = ax + b$. Wówczas mamy, że wielomiany $f$ i $h$ są względnie pierwsze, gdyż $f(-b/a) \neq 0$. Zauważmy również, że

$\deg h(x)(f(x)-h(x)) = n+1$. Ponadto, wielomian $h(x)(f(x)-h(x))$ ma tylko dwa pierwiastki: $x=0$ (rzędu $n$) i $x=-b/a$ (rzędu jeden). Jeśli weźmiemy $n>20$, to $2<n/10$ i widzimy, że dla prawie wszystkich $t\in\mathbb{Q}$ na krzywej $C_t:\ d(t)y^2=f(x)$ leżą co najmniej dwa punkty wymierne $P_1$ i $P_2$. Stoi to w jawnej sprzeczności z tezą Twierdzenia 0.1. □

**Uwaga 0.7.** Stosując skonstruowaną przez nas rodzinę krzywych możemy również obalić Twierdzenie 8 (i) z pracy [3].

Pokazaliśmy, że Twierdzenie 0.1 jest nieprawdziwe. W takiej sytuacji są dwie możliwości: w dowodzie znajduje się błąd lub jedno bądź więcej założeń nie jest prawdziwe (może to mieć miejsce zwłaszcza w przypadku, gdy założenia są nieudowodnionymi hipotezami). Po wymianie korespondencji z Autorem pracy [3] okazało się, że w dowodzie „twierdzenia" znajduje się błąd. Nie był to poważny błąd, raczej rodzaj przeoczenia. W wyniku tej obserwacji Twierdzenie 0.1 udaje się uratować przez dodanie pewnego technicznego założenia. Poprawiona wersja tego twierdzenia brzmi następująco:

**Twierdzenie 0.8 (Poprawiona wersja Twierdzenia 0.1).** *Załóżmy, że hipotezy* abc *i* abcd *są prawdziwe. Niech $f\in\mathbb{Z}[x]$, $\deg f=n$ i załóżmy, że $f$ nie ma pierwiastków wielokrotnych. Jeśli istnieje wielomian $h\in\mathbb{Z}[x]$ względnie pierwszy z $f$ i taki, że $h(x)(f(x)-h(x))$ ma mniej niż $n/10$ różnych pierwiastków, wówczas, dla wszystkich dostatecznie dużych liczb bezkwadratowych $d$, dla których istnieją co najmniej dwa nietrywialne rozwiązania równania $dy^2=f(x)$, powiedzmy $dy_1^2=f(x_1)$ i $dy_2^2=f(x_2)$, gdzie $x_1,x_2\in\mathbb{Q}$, mamy $h(x_1)/f(x_1)=h(x_2)/f(x_2)$ lub $h(x_1)/f(x_1)+h(x_2)/f(x_2)=1$.*

Tę poprawioną wersję można znaleźć w pracy [4].

Nasz kontrprzykład na Twierdzenie 0.1 już nie działa, gdyż jest zawarty w tym dodatkowym warunku. Istotnie, zauważmy na początek, że $at^2T(t)+b=t^{2n}(aT(t)+b)$. Jest to wniosek z definicji funkcji $T=T(t)$ danej przez (3). Otrzymujemy stąd, że

$$\frac{h(t^2T(t))}{f(t^2T(t))}=\frac{at^2T+b}{t^{2n}T^n+at^2T+b}=\frac{t^{2n}(aT+b)}{t^{2n}T^n+t^{2n}(aT+b)}=\frac{aT+b}{T^n+aT+b}=\frac{h(T(t))}{f(T(t))},$$

i nasz kontrprzykład już nim nie jest.

Jest bardzo prawdopodobne, że podczas naszej matematycznej podróży Czytelnik zadał sobie pytanie: dlaczego ktokolwiek miałby wątpić w prawdziwość Twierdzenia 0.1? Zwłaszcza, że twierdzenie to ukazało się w recenzowanym czasopiśmie matematycznym i na pierwszy rzut oka wydaje się bardzo prawdopodobne. Na tak postawione pytanie bardzo trudno odpowiedzieć. Autor niniejszego artykułu, który miał to szczęście, że znalazł zaprezentowany kontrprzykład, zaufał swojej matematycznej intuicji. Czym jest owa intuicja? Matematyczna intuicja to nic innego jak wypadkowa wysłuchanych wykładów, przeczytanych prac oraz własnych rozmyślań i badań matematycznych. Intuicja podpowiedziała Mu, że to „twierdzenie" ... jest zbyt piękne, żeby było prawdziwe. Ta sugestia oraz wiedza wyniesiona z zupełnie innych rozważań pozwoliła intuicję zamienić w konkretny i łatwo weryfikowalny kontrprzykład.

Mamy nadzieję, że przedstawiony przykład nietrywialnego „twierdzenia" matematycznego, które okazało się nieprawdziwe, przekonał Czytelnika, by podczas czytania prac matematycznych wykazywał się ostrożnością i pewną dozą matematycznej nieufności. Jest to zdrowe podejście, gdyż zawsze należy brać pod uwagę tzw. czynnik ludzki. Przecież dowody twierdzeń są pisane przez ludzi, a ludzie nie są nieomylni i niejednokrotnie zdarza się, że jakiś szczegół umyka, lub że w ferworze walki z dowodem wykorzysta się ... równość $2+2=5$ lub jej bardziej wyrafinowane siostry. Rzecz jasna jest jeszcze recenzent, który powinien wyłapać wszystkie błędy i niejasności. Jednakże, recenzent jest również człowiekiem, a zatem i jemu może się zdarzyć przeoczenie lub uznanie czegoś za oczywiste. Z całą pewnością każdy matematyk lub ogólniej – człowiek pracujący naukowo – znalazł dowód co najmniej jednego „twierdzenia". Z drugiej strony

miejmy również wyrozumiałość dla tych niefortunnych omyłek, gdyż, jak mówi znane przysłowie: *„Nie myli się tylko ten, kto nic nie robi”.*

Mamy również nadzieję, że Czytelnik zachęcony zaprezentowanym przykładem postara się sam znaleźć „twierdzenia” w literaturze matematycznej i obnażyć ich słabości znajdując piękne kontrprzykłady. Matematyka z całą pewnością na tym nie straci.

**Literatura**


[1] J. Browkin, *Hipoteza* abc, Delta 6 (2000).
[2] J. Browkin, *Hipoteza* abcd, Delta 6 (2000).
[3] A. Granville, *Rational and integral points on quadratic twists of a given hyperelliptic curve*, Int. Math. Res. Notices 27 (8)(2007) 1-25.
[4] A. Granville, *Corrigendum for ”Rational and integral points on quadratic twists of a given hyperelliptic curve”*, artykuł dostępny pod adresem `http://www.dms.umontreal.ca/ andrew/PDF/hyperellCorr.pdf`
[5] M. Ulas, *Rational points on certain hyperelliptic curves over finite fields*, Bull. Polish Acad. Sci. Math. **55** (2007), 1-8.