Jak pokazać, że coś ma elementarny dowód, nie pokazując elementarnego dowodu

*Leszek KOŁODZIEJCZYK**

Zdarza się, że jakieś ważne twierdzenie dotyczy „przyziemnych" obiektów, np. liczb naturalnych albo skończonych zbiorów, ale wszystkie znane jego dowody odwołują się do zupełnie nieprzyziemnych pojęć i metod. W takich sytuacjach pada czasem pytanie: czy to twierdzenie ma dowód elementarny? „Elementarny" nie znaczy tu ani „łatwy", ani „intuicyjny"; chodzi o dowód, który nie używałby zaawansowanych, abstrakcyjnych pojęć.

W pierwszej połowie XX wieku pytano na przykład, czy istnieje elementarny dowód twierdzenia o asymptotycznej gęstości liczb pierwszych wśród liczb naturalnych. Jak wiadomo, publicznie powątpiewał w to Hardy, niesłusznie zresztą, bo elementarny dowód podał w 1948 r. Selberg (wykorzystując też pewne idee Erdősa). Współcześnie natomiast można się niekiedy zetknąć z pytaniem, czy istnieje elementarny dowód (bądź: jak elementarny może być dowód) wielkiego twierdzenia Fermata.

Pojęcie elementarnego dowodu jest, rzecz jasna, intuicyjne, nieostre i w dodatku stopniowalne. Można je jednak w taki czy inny sposób uściślać. Poniżej opiszemy, jak za pomocą narzędzi logiki matematycznej sformułować jedno z możliwych częściowych uściśleń, a następnie pokazywać, że pewne twierdzenia mają elementarne dowody, przezornie unikając przykrego zajęcia, jakim bywa znajdowanie tych dowodów.

1. Arytmetyka pierwszego rzędu

Arytmetyka Peano, czyli PA, zwana też czasem *arytmetyką pierwszego rzędu*, to teoria aksjomatyczna sformułowana w języku zawierającym symbole $+, \cdot, 0, 1$ oraz $\leqslant$. Aksjomaty PA, mające wyrażać fundamentalne własności liczb naturalnych, dzielą się na dwie grupy. Grupę pierwszą tworzą aksjomaty części nieujemnej pierścienia dyskretnie uporządkowanego, a więc np.: $\forall x\,(0 \leqslant x)$, $\forall x\,(x \cdot 1 = x)$, $\forall x\,(x \leqslant 1 \Rightarrow x = 0 \vee x = 1)$, aksjomaty przemienności dodawania i mnożenia, itd. Grupa druga to aksjomaty indukcji matematycznej. Dla każdej formuły $\varphi(x)$, aksjomatem PA jest formuła

$$\varphi(0) \wedge \forall x\,[\varphi(x) \Rightarrow \varphi(x+1)] \Rightarrow \forall x\,\varphi(x).$$

PA można utożsamić z teorią mnogości ograniczoną do zbiorów skończonych, w następującym sensie: istnieje tłumaczenie formuł języka arytmetyki na język teorii mnogości, przy którym wszystkie aksjomaty PA stają się dowodliwe w teorii $\mathsf{ZFC} \setminus \{\mathsf{Inf}\} + \neg\mathsf{Inf}$, czyli teorii mnogości z aksjomatem nieskończoności zastąpionym jego negacją, oraz odwrotne tłumaczenie języka teorii mnogości na język arytmetyki, przy którym wszystkie aksjomaty $\mathsf{ZFC} \setminus \{\mathsf{Inf}\} + \neg\mathsf{Inf}$ stają się dowodliwe w PA.

Zaznaczmy, że w tym miejscu trzeba być dość ostrożnym i aksjomaty ZFC (Zermelo–Fraenkela) sformułować w odpowiedni sposób. Wzięcie dowolnej podręcznikowej listy aksjomatów i mechaniczne wykreślenie spośród nich aksjomatu nieskończoności może dać teorię patologicznie słabą, która nie dowodzi na przykład, że każdy zbiór ma domknięcie przechodnie. Szczegóły pomijamy, zainteresowanych odsyłając do artykułu [1].

Utożsamienie to ma przynajmniej dwie istotne dla nas konsekwencje. Po pierwsze, w PA można mówić nie tylko o liczbach naturalnych, ale o dowolnych zbiorach skończonych, w tym strukturach kombinatorycznych, takich jak grafy czy słowa. Po drugie, twierdzenia dowodliwe w PA to dokładnie te, które można udowodnić bez odwoływania się do obiektów nieskończonych. Właśnie brak tego rodzaju odwołań uznamy za warunek wystarczający elementarności dowodu. Innymi słowy, przyjmujemy, że jeśli twierdzenie jest dowodliwe w PA, to ma elementarny dowód.

Doświadczenie minionych kilku dziesięcioleci uczy, że klasa twierdzeń, które mają dowody w PA, czyli mają dowody elementarne w naszym rozumieniu tego słowa, jest znacznie szersza niż mogłoby się z początku wydawać. Dowody w PA często wymagają jednak różnego rodzaju kodowań czy aproksymacji i nie zawsze są intuicyjne. Zdecydowanie wygodniej jest rozumować w teorii dysponującej bogatszym zestawem pojęć i szerszą klasą dopuszczalnych metod. Dla nas

*Wydział Matematyki, Informatyki i Mechaniki, Instytut Matematyki, UW, ul. Banacha 2, 02-097 Warszawa, lak@mimuw.edu.pl

szczególnie interesująca jest sytuacja, w której wszystkie twierdzenia wyrażalne w języku PA (a zatem „twierdzenia o obiektach skończonych"), które można udowodnić w takiej bogatszej teorii, mają też dowody w PA. Mówimy wówczas, że dana teoria jest *konserwatywna* nad PA.

2. Arytmetyka drugiego rzędu

Ważnym przykładem teorii bogatszej niż PA jest Z_2, czyli *arytmetyka drugiego rzędu*. Język arytmetyki drugiego rzędu zawiera dwa rodzaje zmiennych: zmienne „pierwszego rzędu" $x, y, z, \ldots$, które w zamierzeniu oznaczają liczby naturalne i zachowują się tak jak zmienne w języku PA, oraz zmienne „drugiego rzędu" $X, Y, Z, \ldots$, które w zamierzeniu oznaczają zbiory liczb naturalnych. W języku jest też jeden nowy symbol pozalogiczny $\in$, oznaczający relację należenia pomiędzy obiektami pierwszego i drugiego rzędu. Najważniejszym nowym składnikiem aksjomatyki jest schemat wyróżniania: dla każdej formuły $\psi(x)$ nie zawierającej zmiennej wolnej Z aksjomatem jest formuła

$$\exists Z\, \forall x\, [x \in Z \Leftrightarrow \psi(x)].$$

Litera Z w oznaczeniu tej teorii wzięła się stąd, że arytmetyka jest o liczbach, a dzieło, w którym arytmetykę drugiego rzędu zdefiniowano, miało tytuł zaczynający się od słowa *Grundlagen*. Arytmetykę Peano oznacza się czasami, dziś już raczej rzadko, symbolem Z_1.

W obecności wyróżniania zasadę indukcji matematycznej można wyrazić za pomocą pojedynczego aksjomatu:

$$\forall X\, [0 \in X \wedge \forall x\, (x \in X \Rightarrow x + 1 \in X) \Rightarrow \forall x\, (x \in X)].$$

Mamy też, jak poprzednio, aksjomaty nieujemnej części pierścienia dyskretnie uporządkowanego.

Język arytmetyki drugiego rzędu ma bardzo dużą siłę wyrazu. Podobnie bowiem jak zmienne pierwszego rzędu mogą reprezentować nie tylko liczby naturalne, ale i na przykład liczby wymierne, albo skończone zbiory czy ciągi liczb, zmienne drugiego rzędu mogą reprezentować nie tylko zbiory liczb naturalnych, ale praktycznie dowolne obiekty matematyczne opisywalne za pomocą przeliczalnej ilości informacji. W języku Z_2 można więc mówić między innymi o nieskończonych ciągach liczb, o liczbach rzeczywistych (jako ciągach Cauchy'ego liczb wymiernych), funkcjach ciągłych z $\mathbb{R}$ w $\mathbb{R}$ (albo z $\mathbb{R}^n$ w $\mathbb{R}^n$), ośrodkowych przestrzeniach metrycznych, otwartych, domkniętych czy nawet dowolnych borelowskich podzbiorach tychże, przeliczalnych strukturach algebraicznych itd.

W arytmetyce drugiego rzędu można nie tylko bardzo dużo wyrazić, ale i dużo udowodnić. Praktyka pokazuje, że niemal każde twierdzenie, z którym można się zetknąć w ciągu pierwszych kilku lat studiów matematycznych, można udowodnić w Z_2, jeśli tylko można je w ogóle wysłowić w jej języku. O przykłady twierdzeń wyrażalnych, lecz niedowodliwych w Z_2 (a dowodliwych w ZFC) wcale nie tak łatwo: być może najlepszym jest twierdzenie Martina o determinacji gier borelowskich.

Oczywiście, jest wiele twierdzeń, które można wyrazić w języku arytmetyki drugiego rzędu tylko po dokonaniu stosownych ograniczeń. Przykładowo, twierdzenie Hahna-Banacha w pełnej wersji nie jest wyrażalne; twierdzenie Hahna-Banacha dla ośrodkowych przestrzeni Banacha jest już nie tylko wyrażalne, ale i dowodliwe.

Z naszego punktu widzenia Z_2 jest wręcz teorią zbyt silną, nie jest bowiem konserwatywna nad PA. Świadczy o tym między innymi zdanie $\mathsf{Con}_{\mathsf{PA}}$ wyrażające niesprzeczność PA. Na mocy drugiego twierdzenia Gödla, $\mathsf{Con}_{\mathsf{PA}}$ nie ma dowodu w PA, a w Z_2 może być udowodnione za pomocą bardzo prostego rozumowania: zbiór wszystkich liczb naturalnych ze zwykłymi działaniami spełnia wszystkie aksjomaty PA, toteż PA nie może być sprzeczna. Jeśli $\mathsf{Con}_{\mathsf{PA}}$ uznać za zdanie „nie dość matematyczne, by się nim przejmować", jako przykłady twierdzeń świadczących o niekonserwatywności Z_2 nad PA mogą służyć między innymi twierdzenie Parisa-Harringtona (będące wzmocnieniem skończonego twierdzenia Ramseya), twierdzenie Goodsteina (mówiące o tym, że pewne specyficzne ciągi liczb naturalnych są skończone) albo rozmaite konsekwencje grafowego twierdzenia o minorach.

3. Pewien przykład konserwatywności

Rozważymy teraz pewien ważny fragment Z_2. Teorię ACA_0 definiuje się podobnie jak Z_2, ograniczając jednak schemat wyróżniania do formuł *arytmetycznych*, czyli nie zawierających kwantyfikacji po zmiennych drugiego rzędu. Aksjomaty

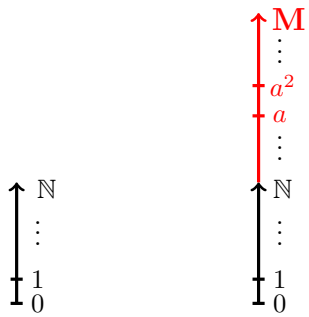
Skrót ACA oznacza Arithmetical Comprehension Axiom.

ACA_0 gwarantują więc istnienie np. zbioru liczb pierwszych, a dla danego częściowego porządku $(X, \preceq)$ gwarantują istnienie zbioru tych $x \in X$, dla których zbiór $\{y \in X : y \preceq x\}$ jest nieskończony (bo kwantyfikacja „dla każdej skończonej listy elementów istnieje element spoza tej listy" jest pierwszego rzędu). Nie ma natomiast gwarancji, że istnieje zbiór tych x, dla których $\preceq$ ograniczone do $\{y \in X : y \preceq x\}$ nie jest dobrym porządkiem (bo „istnieje nieskończony ciąg zstępujący" jest drugiego rzędu).

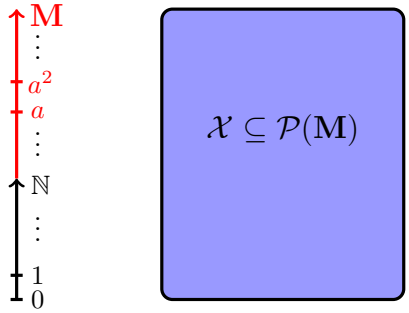
Okazuje się, że zachodzi

Twierdzenie (H. Friedman)**.** ACA_0 *jest konserwatywne nad* PA*.*

Dowodów powyższego twierdzenia o konserwatywności jest kilka. Rozumowanie, które tu opiszemy, wyróżnia się szczególną prostotą, ale wymaga użycia modeli arytmetyki, o których musimy w związku z tym parę słów powiedzieć. Przypomnijmy, że model teorii aksjomatycznej T to po prostu struktura, która spełnia wszystkie aksjomaty T. *Twierdzenie o pełności* orzeka, że dane zdanie ψ da się udowodnić w teorii T dokładnie wtedy, gdy każdy model T spełnia również ψ.



Modele PA to oczywiście części nieujemne pewnych (bardzo szczególnych) pierścieni dyskretnie uporządkowanych. PA ma jeden (z dokładnością do izomorfizmu) model *standardowy*, czyli zwykłe liczby naturalne (narysowane schematycznie z lewej) oraz mnóstwo modeli *niestandardowych*, wyglądających mniej więcej tak, jak na rysunku z prawej: każdy model niestandardowy ma odcinek początkowy izomorficzny ze zwykłymi liczbami naturalnymi, a powyżej niego *elementy niestandardowe*, takie jak a na rysunku.



Model Z_2 albo ACA_0 składa się natomiast z *części pierwszego rzędu*, M, która jest po prostu modelem PA, oraz *części drugiego rzędu*, $\mathcal{X}$, która jest pewną podrodziną $\mathcal{P}(\mathrm{M})$. Można to zobaczyć mniej więcej tak, jak widać na rysunku obok.

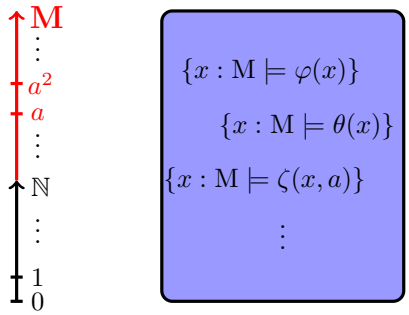
Oczywiście, rodzina $\mathcal{X}$ nie może być zupełnie byle jakim podzbiorem $\mathcal{P}(\mathrm{M})$, choćby dlatego, że musi spełniać odpowiednie aksjomaty wyróżniania. Ważne jest jednak, że w ogólności może zachodzić $\mathcal{X} \neq \mathcal{P}(\mathrm{M})$.

Twierdzenie o konserwatywności ACA_0 nad PA jest łatwym wnioskiem z następującego lematu:

Lemat. *Każdy model* PA *jest częścią pierwszego rzędu pewnego modelu* ACA_0*.*

Załóżmy bowiem, że konserwatywności nie ma, czyli że jest zdanie ψ w języku arytmetyki pierwszego rzędu dowodliwe w ACA_0, ale nie w PA. Na mocy twierdzenia o pełności, istnieje struktura M spełniająca PA, w której zachodzi $\neg\psi$. Z lematu wiemy, że M jest częścią pierwszego rzędu pewnego modelu ACA_0. W modelu tym $\neg\psi$ nadal musi być spełnione, bo wartość logiczna $\neg\psi$ zależy wyłącznie od części pierwszego rzędu! To jest już jednak sprzeczne z założeniem, że ACA_0 dowodzi ψ.

Sam dowód lematu jest również nietrudny. Rozważmy model M spełniający PA. Jako $\mathcal{X}$ weźmy $\mathrm{Def}(\mathrm{M})$, czyli rodzinę wszystkich tych podzbiorów M, które można zdefiniować jakąś formułą języka PA, być może zawierającą parametry z M.



Każdy element Def(M) jest więc postaci $\{x : \mathrm{M} \models \psi(x, a_1, \ldots, a_n)\}$, gdzie ψ jest pewną formułą arytmetyki pierwszego rzędu, $a_1, \ldots, a_n$ są elementami M, a dla $x \in \mathrm{M}$ zapis $\mathrm{M} \models \psi(x, a_1, \ldots, a_n)$ oznacza, że elementy $x, a_1, \ldots, a_n$ spełniają w M formułę ψ.

Czyli jest tak, jak na rysunku obok.

Przekonajmy się, że para $(\mathrm{M}, \mathrm{Def}(\mathrm{M}))$ jest modelem ACA_0. To, że M spełnia aksjomaty pierścienia dyskretnie uporządkowanego, wiemy z założenia.

Trzeba natomiast sprawdzić, że w $(\mathrm{M}, \mathrm{Def}(\mathrm{M}))$ spełniony jest aksjomat wyróżniania dla dowolnej formuły nie zawierającej kwantyfikatorów drugiego rzędu. Drobna subtelność polega na tym, że formuła może zawierać (nieskwantyfikowane) parametry drugiego rzędu. Niech $\psi(x)$ będzie taką formułą, a $Y_1, \ldots, Y_n$ występującymi w niej parametrami drugiego rzędu. Ponieważ $Y_1, \ldots, Y_n \in \mathrm{Def}(\mathrm{M})$, istnieją formuły $\varphi_1, \ldots, \varphi_n$ w języku PA takie, że dla $i = 1, \ldots, n$ zachodzi $Y_i = \{y : \mathrm{M} \models \varphi_i(y)\}$. Formuły φ_i również mogą zawierać parametry, ale już tylko pierwszego rzędu.

W takim razie jednak zbiór tych $x \in \mathrm{M}$, dla których zachodzi $\psi(x, Y_1, \ldots, Y_n)$, jest dokładnie równy

$$\{x : \mathrm{M} \models \psi(x, \varphi_1, \ldots, \varphi_n)\},$$

gdzie formuła $\psi(x, \varphi_1, \ldots, \varphi_n)$ powstaje z ψ przez wstawienie w miejsce każdego z parametrów Y_i jego definicji, czyli formuły φ_i. Zbiór $\{x : \mathrm{M} \models \psi(x, \varphi_1, \ldots, \varphi_n)\}$ oczywiście należy do Def(M), gwarantując spełnienie rozważanego aksjomatu wyróżniania.

Pozostaje sprawdzić, że $(\mathrm{M}, \mathrm{Def}(\mathrm{M}))$ spełnia aksjomat indukcji matematycznej. Jeśli $X \in \mathrm{Def}(\mathrm{M})$, to X jest pozdbiorem M zdefiniowanym pewną formułą φ. Jeśli $0 \in X$ i $\forall x\,(x \in X \Rightarrow x + 1 \in X)$, to M spełnia $\varphi(0) \wedge \forall x\,[\varphi(x) \Rightarrow \varphi(x + 1)]$. Z aksjomatów PA wnioskujemy zatem, że M spełnia $\forall x\,\varphi(x)$, z czego natychmiast wynika, iż wszystkie elementy $x \in M$ należą do zbioru X.

To kończy dowód lematu, a zatem dowód twierdzenia o konserwatywności.

4. Które metody się „elementaryzują”?

Z konserwatywności ACA_0 nad PA wynika, że każde twierdzenie, które jesteśmy w stanie udowodnić, rozumując w arytmetyce drugiego rzędu i dbając, by nie używać schematu wyróżniania dla zbyt skomplikowanych formuł, ma również dowód elementarny. Otrzymaliśmy więc pewne narzędzie służące do pokazywania, że rozmaite wyniki można udowodnić elementarnie, bez konieczności konstruowania ich elementarnych dowodów. By się przekonać, w jakim stopniu jest to narzędzie skuteczne, trzeba zrozumieć, jak dużą klasą metod można się posługiwać w ACA_0.

Oczywiście, z góry wiadomo, że ACA_0 musi być istotnie słabsza niż pełna arytmetyka drugiego rzędu, choćby właśnie dlatego, że jest konserwatywna nad PA. Najbardziej uderzającą słabością ACA_0 jest niezdolność do udowodnienia podstawowych faktów na temat dobrych porządków, a co za tym idzie, niezdolność do posługiwania się nieskończonymi liczbami porządkowymi. Wskutek tego, ACA_0 nie dowodzi na przykład twierdzenia Cantora-Bendixsona, jak również różnych innych twierdzeń (m.in. o strukturze przeliczalnych grup abelowych), których dowody wymagają użycia indukcji pozaskończonej. ACA_0 niezbyt dobrze radzi sobie także z niektórymi zaawansowanymi metodami teorii Ramseya i zdecydowaną większością metod teorii dobrych quasi-porządków.

W celu zilustrowania, jakiego rodzaju argumentację da się dla odmiany przeprowadzić w ACA_0, naszkicujemy (bez przesadnej dbałości o formalne szczegóły) dowód prostego a ważnego wyniku, jakim jest twierdzenie Bolzano-Weierstrassa. Mamy pokazać, że każdy ciąg liczb rzeczywistych z przedziału $[0, 1]$ ma podciąg zbieżny. Rozważmy więc taki ciąg, powiedzmy $(r_n)_{n \in \mathbb{N}}$. Ponieważ liczby rzeczywiste są dla nas ciągami Cauchy'ego liczb

wymiernych, $(r_n)_{n\in\mathbb{N}}$ jest z formalnego punktu widzenia podwójnie indeksowanym ciągiem liczb wymiernych.

Dla $k \in \mathbb{N}$, niech s_k równa się $\frac{p_k}{2^k}$, gdzie p_k jest największą liczbą spośród $\{0, \ldots, 2^k - 1\}$, dla której w przedziale $[\frac{p_k}{2^k}, \frac{p_k+1}{2^k}]$ jest nieskończenie wiele r_n-ów. ACA_0 nie ma najmniejszych problemów ze sprawdzeniem, że ciąg $(s_k)_{k\in\mathbb{N}}$, jeśli tylko istnieje, jest ciągiem Cauchy'ego, a zatem reprezentuje pewną liczbę rzeczywistą s. Istnienie ciągu $(s_k)_{k\in\mathbb{N}}$ wynika natomiast ze schematu wyróżniania dla formuł arytmetycznych, gdyż, po pierwsze, "istnieje nieskończenie wiele n" można wyrazić za pomocą kwantyfikacji pierwszego rzędu: „dla każdego m istnieje $n \geqslant m$"; po drugie zaś, dla danego n oraz danych liczb wymiernych p, q, formuła „$r_n \in [p, q]$" również wymaga tylko kwantyfikacji pierwszego rzędu: „dla dowolnie dużych m i dla dostatecznie dużych ℓ, ℓ-ty wyraz ciągu reprezentującego r_n jest pomiędzy $p - \frac{1}{m}$ a $q + \frac{1}{m}$".

Zdefiniujmy teraz podciąg $(r_{n_k})_{k\in\mathbb{N}}$ ciągu $(r_n)_{n\in\mathbb{N}}$ w następujący sposób: $(n_0, \ldots, n_k)$ ma być leksykograficznie najmniejszym rosnącym ciągiem indeksów długości $k + 1$, dla którego $|s - r_{n_i}| \leqslant 2^{-i}$ jest spełnione dla wszystkich $i \leqslant k$. Znów okazuje się, że do zdefiniowania ciągu $(r_{n_k})_{k\in\mathbb{N}}$ wystarcza kwantyfikacja pierwszego rzędu, a więc ten ciąg istnieje. Bez trudu sprawdzamy, że ciąg $(r_{n_k})_{k\in\mathbb{N}}$ dąży do s, co kończy dowód.

Twierdzenie Bolzano-Weierstrassa jest, rzecz jasna, tylko nader prostym przykładem. Badania w ramach *matematyki odwrotnej*, czyli programu klasyfikowania siły logicznej twierdzeń matematycznych za pomocą fragmentów arytmetyki drugiego rzędu, pokazały jednak, że w ACA_0 można sformalizować bardzo dużą część klasycznej matematyki. Wśród przykładów wyników dowodliwych w ACA_0, które podaje S. Simpson w podstawowej monografii na temat matematyki odwrotnej, czyli książce [2], są między innymi:

- podstawowe twierdzenia na temat funkcji ciągłych oraz rachunku różniczkowego i całkowego jednej i wielu zmiennych, z którymi można zetknąć się na typowym kursie analizy matematycznej,
- twierdzenie Arzeli-Ascolego,
- twierdzenie Peano o istnieniu rozwiązań równań różniczkowych zwyczajnych,
- twierdzenie Baire'a o kategoriach dla ośrodkowych przestrzeni zupełnych,
- twierdzenie Brouwera o punkcie stałym,
- istnienie ideałów maksymalnych w przeliczalnym pierścieniu,
- istnienie i jedyność algebraicznego domknięcia ciała przeliczalnego,
- twierdzenia Banacha-Steinhausa i Hahna-Banacha dla ośrodkowych przestrzeni Banacha,
- lemat Königa,
- twierdzenie o pełności.

Należy przy tym mieć świadomość, że nie są to izolowane przykłady. Każdy wynik typu „takie-a-takie twierdzenie jest dowodliwe w ACA_0" niesie w istocie informację: „taka-a-taka klasa metod używanych w określonej dziedzinie formalizuje się w ACA_0". Powyższe przykłady informują więc, że w ACA_0 można używać między innymi wielu klasycznych metod analizy rzeczywistej, algebry struktur przeliczalnych, a także analizy funkcjonalnej i topologii przestrzeni ośrodkowych. Wiadomo również, że to samo dotyczy także analizy zespolonej, z jakichś powodów zaniedbanej w pracach z okresu podsumowanego książką Simpsona. ACA_0 posługuje się podstawowymi technikami analizy zespolonej w stopniu, który między innymi z nadwyżką wystarcza do tego, by bez większego trudu odtworzyć dowód twierdzenia o liczbach pierwszych.

Efekty badań nad siłą ACA_0, w połączeniu z twierdzeniem o konserwatywności nad PA, można podsumować następująco: jeśli jakieś twierdzenie z teorii liczb czy kombinatoryki ma dowód używający w miarę tradycyjnych metod, nie wymagający narzędzi typowo teoriomnogościowych ani definiowania szczególnie skomplikowanych zbiorów, jest bardzo duża szansa na to, że ma ono dowód elementarny. Dla Hardy'ego byłoby to zaskoczenie.

5. A ponadto...

Na zakończenie wspomnijmy jeszcze o dwu zasługujących na wzmiankę kwestiach.

Jako zdania klasy Π^0_2 można sformułować między innymi hipotezę liczb pierwszych bliźniaczych czy $\mathrm{P} \neq \mathrm{NP}$, a w jeszcze prostszej postaci można wyrazić na przykład wielkie twierdzenie Fermata, hipotezę Goldbacha czy nawet hipotezę Riemanna.

Po pierwsze, niekiedy od dowodu chciałoby się więcej niż samej tylko elementarności. Rozważmy dla przykładu zdania klasy Π^0_2, czyli postaci $\forall x\, \exists y\, \psi(x, y)$, gdzie x, y to zmienne arytmetyki pierwszego rzędu, a ψ jest formułą, w której występuje już tylko kwantyfikacja ograniczona, w rodzaju $\exists z \leqslant x^2 + y$. Bardzo wiele ważnych dla matematyki zdań jest takiej postaci. Można by sobie życzyć, aby dowód zdania klasy Π^0_2 zawierał opis algorytmu znajdującego y na wejściu x — lepszego niż samo „przeszukuj wszystkie y, aż trafisz na takie, dla którego zachodzi $\psi(x, y)$". Okazuje się, że gwarancją istnienia takiego algorytmicznego dowodu jest dowodliwość w pewnych nietrywialnych podteoriach ACA_0. Najważniejsza teoria tego rodzaju, znana jako WKL_0, powstaje przez nieco drastyczniejsze niż w przypadku ACA_0 ograniczenie schematu wyróżniania oraz dodanie osobnego (dowodliwego w ACA_0) aksjomatu mówiącego, że przedział $[0, 1]$ jest zwarty w sensie pokryć zbiorami otwartymi. Co ciekawe, WKL_0 nie dowodzi twierdzenia Bolzano-Weierstrassa. Nie dowodzi też twierdzenia Arzeli-Ascolego; dowodzi natomiast wszystkich innych twierdzeń z analizy i analizy funkcjonalnej podanych wyżej jako przykłady twierdzeń dowodliwych w ACA_0. Wielu twierdzeń z algebry i innych dziedzin WKL_0 dowodzi w słabszych wersjach: nie potrafi na przykład pokazać, że w każdym przeliczalnym pierścieniu jest ideał maksymalny, ale potrafi zawsze znaleźć ideał pierwszy.

Po drugie, powyżej staraliśmy się podkreślać, że twierdzenie o konserwatywności ACA_0 nad PA pozwala stwierdzić istnienie pewnych dowodów elementarnych bez ich konstruowania. Nasuwa się pytanie, czy tych dowodów nie dałoby się jednak skonstruować. Czy nie można by na przykład podać jawnego tłumaczenia dowodów w ACA_0 na dowody w PA?

Takie tłumaczenie istnieje, ale wymaga uprzedniego poddania dowodu w ACA_0 syntaktycznej procedurze zwanej *eliminacją cięcia*, która skutkuje między innymi olbrzymim wzrostem rozmiaru dowodu. Wiadomo, że istnieje stała c o następującej własności: dla każdego n istnieje twierdzenie dowodliwe w PA, które w ACA_0 ma pewien dowód rozmiaru co najwyżej cn, podczas gdy wszystkie dowody w PA wymagają rozmiaru przynajmniej

$$2^{2^{\cdot^{\cdot^{\cdot^{2}}}}},$$

gdzie wysokość wieży jest równa n. Być może pracowite konstruowanie tych dowodów jednak nie jest najlepszym pomysłem.

Literatura

[1] Richard Kaye and Tin Lok Wong. *On interpretations of arithmetic and set theory*. Notre Dame Journal of Formal Logic, 48(4):497–510, 2007.

[2] Stephen G. Simpson. *Subsystems of Second Order Arithmetic*. Association for Symbolic Logic, 2009.