Jest to zapis odczytu wygłoszonego na XXVIII Szkole Matematyki Poglądowej „Pomysły", Grzegorzewice, styczeń 2002

Twierdzenie Kurta Gödla

Wiktor BARTOL, Warszawa

Wiek XIX, wiek narodzin nowoczesnej matematyki, dostarczył wielu okazji do głębokiego namysłu nad jej sensem i logicznymi podstawami. Powstanie geometrii nieeuklidesowych pobudziło refleksje dotyczące relacji i różnic między rzeczywistością a założeniami teorii matematycznej, aksjomatyzacja arytmetyki przez Giuseppe Peano (1891) i geometrii przez Davida Hilberta (1899) zachęcały do wejścia na drogę budowy fundamentów matematyki wolnych od subiektywnych przekonań o prawdzie przyjmowanych twierdzeń, pojawiające się coraz częściej na przełomie wieków paradoksy logiczne i semantyczne wskazywały na niebezpieczeństwa tkwiące w nie dość formalnym opisie badanych obiektów. Prace Gottloba Fregego z końca XIX wieku oraz *Principia Mathematica* Bertranda Russella i Alfreda Whiteheada z początków XX wieku sugerowały możliwości zanurzenia matematyki w systemie logiki formalnej.

Nic dziwnego, że w początkach XX wieku zrodziły się nadzieje na oparcie całej matematyki na solidnych podstawach aksjomatycznych i wyprowadzania wszystkich twierdzeń za pomocą ustalonych, sformalizowanych logicznych reguł wnioskowania, niezależnych od wszelkich uwarunkowań psychologicznych. David Hilbert, który swoje zainteresowanie taką wizją wyraził nie tylko poprzez aksjomatyzację geometrii, ale także w postaci jednego z problemów przedłożonych II Międzynarodowemu Kongresowi Matematyków w 1900 roku, postulując aksjomatyzację matematycznych podstaw fizyki, sformułował w początkach XX wieku dalekosiężny program. Ów *program Hilberta* miał przeorać całą matematykę, zamienić ją niemal w grę podobną szachom, gdzie dozwolone są tylko bardzo precyzyjnie określone ruchy, a sens, jaki może chcieć nadawać figurom gracz, pozostaje jego osobistą sprawą, nie wpływając w żaden sposób na reguły gry. Nagrodą za wysiłek prowadzący do tego celu miała być matematyka pewna i niesprzeczna, której twierdzenia – z twierdzeniem o niesprzeczności włącznie – można wyprowadzić z aksjomatów w skończonej liczbie kroków za pomocą "precyzyjnie określonych ruchów".

Wizja Hilberta zaowocowała rozwojem badań nad podstawami matematyki, ale program Hilberta okazał się nazbyt optymistyczny. Wykazał to Kurt Gödel w pracy ogłoszonej w 1930 roku, a opublikowanej rok później. Praca nosiła tytuł *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I* (O formalnie nierozstrzygalnych zdaniach *Principia Mathematica* i systemów pokrewnych), a jej głównymi wynikami były dwie własności niesprzecznych systemów formalnych, zawierających arytmetykę liczb naturalnych. Pierwsze stwierdzało, że w każdym takim systemie istnieje zdanie nierozstrzygalne, a więc takie, którego na gruncie tego systemu nie można ani udowodnić, ani obalić (czyli udowodnić zdania do niego przeciwnego). System o tej własności nazywa się *niezupełnym*; pierwsze twierdzenie ustanawiało zatem niezupełność arytmetyki liczb naturalnych (jeśli jest nieprzeczna). Drugie orzekało, że środkami takiego systemu, wewnątrz niego, jego własnej niesprzeczności udowodnić nie można.

Historia myśli ludzkiej zna wiele przykładów paradoksów logicznych, których istotą jest szczególnego rodzaju zapętlenie: zdanie orzekające samo o sobie. Poczynając od Eubulidesa (IV w.p.n.e.) i paradoksu kłamcy (mówiąc "kłamię", kłamię czy mówię prawdę?) aż po paradoks Richarda z 1905 roku przewijał się wątek stosunku języka do metajęzyka, poprawności sformułowań i definicji itp. Przyjrzyjmy się ostatniemu paradoksowi, który zawdzięczamy matematykowi francuskiemu Julesowi Richardowi. Rozważmy wszystkie definicje arytmetycznych własności liczb naturalnych. Używając skończenie wielu znaków do ich zapisu, mamy takich definicji co najwyżej przeliczalnie wiele i możemy je uporządkować według długości (najkrótsze na początek), przyjmując w ramach grupy definicji o tej samej długości porządek leksykograficzny, określony przez pewien porządek liniowy na zbiorze znaków. Przypisując każdej z tak ustawionych definicji kolejny numer (liczbę naturalną), potrafimy rozróżnić dwie kategorie liczb: te, które mają własność reprezentowaną przez przypisaną im definicję, i te, które nie mają własności reprezentowanej przez przypisaną im definicję. Te ostatnie nazwijmy *liczbami Richardowskimi*. Na przykład, gdyby własność bycia liczbą parzystą nosiła numer 35, liczba 35 byłaby liczbą Richardowską, jako że sama nie jest liczbą parzystą. Załóżmy teraz, że n jest numerem własności bycia liczbą Richardowską. Czy n ma tę własność? Jeśli tak, to znaczy jeśli przysługuje jej własność bycia liczbą Richardowską, to zgodnie z definicją taką liczbą nie jest. Jeśli odwrotnie – n nie ma własności, której jest numerem, a więc nie jest liczbą Richardowską, to – znów zgodnie z definicją takiej liczby – jest liczbą Richardowską. Tak czy owak, sprzeczność.

Oto, zdawałoby się, dobry przykład zdania, którego teoria nie potrafi rozstrzygnąć. Uważny Czytelnik zauważył jednak z pewnością w tym rozumowaniu pewną niekonsekwencję: własność bycia liczbą Richardowską nie jest własnością arytmetyczną, zależy bowiem od ponumerowania napisów, nie mówiąc o tym, że nie napisy, lecz liczby są przedmiotem badań arytmetyki. Gdyby jednak udało się wyrazić napisy za pomocą liczb i znaleźć własność podobną do Richardowskiej, ale arytmetyczną? Gödel dostrzegł taką drogę.

Jeśli przedmiotem rozważań ma być system formalny, jeśli chcemy dowieść pewnej własności takiego systemu, jak niezupełność, to pierwszy krok musi polegać na dokładnym jego opisie, a więc określeniu języka, aksjomatów i reguł wnioskowania. Dokładna postać aksjomatów i reguł wnioskowania nie ma tu szczególnego znaczenia, w każdym razie Gödel, rzecz jasna, wypisał i jedne, i drugie, czerpiąc z*Principia Mathematica* aksjomaty dla teorii liczb naturalnych oraz aksjomaty logiczne niezbędne do zbudowania systemu arytmetyki Peano (PA) i przyjmując jako jedną z reguł wnioskowania regułę odrywania. Zatrzymajmy się natomiast przy opisie języka, gdyż kluczem do sprawy jest możliwość reprezentowania jego wyrażeń za pomocą liczb. Alfabet języka składa się z siedmiu symboli stałych: "0", "s", " $\sim$ ", " $\vee$ ", "$\forall$", "(", ")" oraz ze zbioru zmiennych pierwszego rzędu, czyli indywiduowych (reprezentujących liczby naturalne) i zbioru zmiennych n-tego rzędu dla każdej dodatniej liczby naturalnej n (dla $n > 1$ reprezentujących zbiory obiektów rzędu $n - 1$). Słowa i zdania języka, termy i formuły, budowane są zgodnie z powszechnie dziś znanymi regułami. Interpretacja symboli w systemie formalnym nie ma znaczenia, ale nietrudno zauważyć, że sugestywnie oznaczone symbole stałe odpowiadają kolejno: liczbie zero, funkcji następnika, negacji, alternatywie, kwantyfikatorowi ogólnemu oraz obydwu nawiasom.

Zasadniczy pomysł Gödla polegał na jednoznacznym zakodowaniu wyrażeń języka za pomocą liczb naturalnych; termy i formuły stawały się w ten sposób liczbami i tak jak liczby (mówiąc z pedantyczną ścisłością – nazwy liczb) mogły same być opisywane przez inne formuły. (Czy przymiotnik "inne" jest tu konieczny? Czy formuła nie może opisywać samej siebie?) Przypiszmy więc liczby symbolom języka:

Symbol	Liczba
0	1
s	3
$\sim$	5
$\vee$	7
$\forall$	9
(	11
)	13

Zmiennym indywiduowym przyporządkowujemy kolejne liczby pierwsze, większe od 13: zmiennej x – 17, zmiennej y – 19 itd.; dla $n > 1$, zmiennym rzędu n przyporządkowujemy kolejno n-te potęgi liczb pierwszych większych od 13. W ten sposób przypisaliśmy wzajemnie jednoznacznie liczbę każdemu symbolowi alfabetu. Będziemy ją nazywać *numerem* tego symbolu.

Każda formuła jest ciągiem symboli, należących do alfabetu. Jeśli formuła α zawiera, kolejno, symbole o numerach $n_1, n_2, \ldots, n_k$, to samej formule α

przyporządkujemy numer $2^{n_1}3^{n_2}\dots p_k^{n_k}$, gdzie p_k oznacza k-tą liczbę pierwszą. Z kolei dowód jest ciągiem formuł, więc można się już domyślać, jaki numer przypiszemy takiemu, powiedzmy, l-elementowemu ciągowi formuł: jeśli kolejne formuły mają numery $m_1, m_2, \dots, m_l$, to cały ciąg będzie miał numer $2^{m_1}3^{m_2}\dots p_l^{m_l}$. Tak więc każdy symbol alfabetu, każdy term, każda formuła i każdy ciąg formuł (w szczególności każdy dowód) są reprezentowane przez liczbę (zwaną *numerem Gödlowskim* tego wyrażenia) i to tak, że z danej liczby można jednoznacznie odtworzyć oryginalne wyrażenie. Łatwo zauważyć, że nie każda liczba naturalna jest numerem Gödlowskim, ponieważ istnieje mnóstwo liczb naturalnych różnych od 1, 3, 5, 7, 9, 11 i 13, nie będących potęgą liczby pierwszej i nie mających w rozkładzie na czynniki pierwsze wszystkich liczb pierwszych od 2 do swojego największego dzielnika pierwszego.

Kodowanie formuł i ciągów formuł za pomocą liczb nasuwa skojarzenia z płaszczyzną kartezjańską, której każdy punkt jest opisany jednoznacznie przez parę liczb rzeczywistych. To jednak nie wystarcza, by uznać taką płaszczyznę za instrument użyteczny: trzeba jeszcze przetłumaczyć własności geometryczne na algebraiczne, by móc na gruncie algebry rozwiązywać problemy geometryczne. Podobnie w naszym przypadku: własności metamatematyczne systemu należy przetłumaczyć na język arytmetyki. Gödel wprowadza 45 relacji i funkcji rekurencyjnych, dzięki którym można zapisać o formuły metamatematyczne w języku arytmetyki. Oto niektóre z nich, z małymi wyjątkami w zapisie oryginalnym. Ilustrują one metodę, pozwalającą m.in. wyrażać własności metamatematyczne jako własności liczb naturalnych.

$\mathbf{Z}(n)$ – $ss\dots s0$ (n razy);
$y|x$ – y jest dzielnikiem x);
$\mathbf{Prim}(x)$ – x jest liczbą pierwszą);
$n\mathbf{Pr}x$ – n-ty (w porządku rosnącym) czynnik pierwszy w x);
$\mathbf{Pr}(n)$ – n-ta liczba pierwsza);
$n\mathbf{Gl}x$ – numer symbolu (formuły) stojącego w formule (ciągu) na n-tym miejscu; np. dla $x = 2^{n_1}3^{n_2}\dots p_k^{n_k}$ i $k > 5$, $5\mathbf{Gl}x{=}n_5$);
$x * y$ – z liczb $x = 2^{n_1}3^{n_2}\dots p_k^{n_k}$ i $y = 2^{m_1}3^{m_2}\dots p_l^{m_l}$ tworzy ciąg $2^{n_1}3^{n_2}\dots p_k^{n_k}p_{k+1}^{m_1}p_{k+2}^{m_2}\dots p_{k+l}^{m_l}$);
$\mathbf{Elf}(x)$ – x jest numerem formuły elementarnej);
$\mathbf{Form}(x)$ – x jest numerem formuły);
$\mathbf{Sb}(x, v,\ \mathbf{Z}(y))$ – w formule o numerze x zastępujemy zmienną o numerze v przez Z(y); Sb(x, v,Z(y)) jest liczbą, numerem otrzymanej w ten sposób formuły);
$\mathbf{B}(x)$ – x jest numerem dowodu (czyli liczbą reprezentującą ciąg formuł, będący dowodem));
$\mathbf{Bew}(x, y)$ – x jest numerem dowodu formuły o numerze y).

Podobnie można zapisać aksjomaty Peano, podstawienia aksjomatów logicznych i reguły wnioskowania.

Dobór (przypomnijmy, przedstawiony tu tylko w części) nie jest, rzecz jasna, przypadkowy, pozwala bowiem na udowodnienie twierdzenia, wskazującego na to, że "tłumaczenie" jest wystarczająco pełne.

Twierdzenie. Każda n-argumentowa relacja R rekurencyjna w $\mathbf{N}$ jest reprezentowana przez n-argumentowy symbol relacyjny r, taki że dla dowolnych liczb $x_1, x_2, \dots, x_n$,

1. jeśli $R(x_1, x_2, \dots, x_n)$, to istnieje dowód zdania $r(Z(x_1), \dots, Z(x_n))$,
2. jeśli $\sim R(x_1, x_2, \dots, x_n)$, to istnieje dowód zdania $\sim r(Z(x_1), \dots, Z(x_n))$.

Dowód twierdzenia (jak pisze Gödel) "nie przedstawia trudności zasadniczych, ale jest dość żmudny" i polega na indukcji względem budowy relacji rekurencyjnej.

Przyjrzyjmy się bliżej ostatniej pozycji z naszej skróconej listy. Formułę "Bew(x, y)", określającą pewną relację rekurencyjną między liczbami naturalnymi, możemy interpretować tak: ciąg formuł o numerze x jest dowodem formuły o numerze y. W takim razie formuła

$$\forall x \sim (\mathbf{Bew}(x, y)) \tag{1}$$

reprezentuje zdanie stwierdzające, że żaden ciąg formuł nie jest dowodem formuły o numerze y. Rozpatrzmy szczególny przypadek tego typu formuły, mianowicie:

$$\forall x \sim (\mathbf{Bew}(x, \mathbf{Sb}(y, 19, \mathbf{Z}(y))), \tag{2}$$

powstałej przez wpisanie w poprzedniej formule liczby (ściślej mówiąc, nazwy liczby) $\mathrm{Sb}(y, 19, \mathrm{Z}(y))$. Tak zbudowane wyrażenie ma swój numer Gödlowski, powiedzmy, n. Jaki numer ma wtedy formuła

$$\forall x \sim (\mathbf{Bew}(x, \mathbf{Sb}(n, 19, \mathbf{Z}(n)))? \tag{g}$$

Zauważmy, że $\mathrm{Sb}(n, 19, n)$ jest numerem formuły, która powstała z formuły o numerze n przez zastąpienie w niej zmiennej o numerze 19 (zmiennej y) nazwą liczby n. To jest właśnie zdanie g! Tak więc formuła g reprezentuje zdanie następujące: formuła g nie ma dowodu.

Otóż ta formuła *nie ma* dowodu – jeśli tylko system jest niesprzeczny. Istotnie, gdyby istniał jej dowód, to, jak wykazuje Gödel, istniałby także dowód zdania, które to stwierdza (przypomnijmy, w języku arytmetyki):

$$\sim \forall x \sim (\mathbf{Bew}(x, \mathbf{Sb}(n, 19, \mathbf{Z}(n))).$$

Ale to jest dokładnie zaprzeczenie zdania g! Zatem jeśli istnieje dowód g, to istnieje także dowód zdania przeciwnego. System formalny, w którym istnieje dowód pewnego zdania ϕ oraz istnieje dowód zdania $\sim \phi$, jest systemem sprzecznym. Zatem jeśli arytmetyka Peano oparta na systemie logicznym *Principia Mathematica* jest systemem niesprzecznym, to formuła g nie może mieć, nie ma dowodu w tym systemie. Załóżmy teraz, że istnieje w tym systemie dowód zaprzeczenia formuły g, czyli zdania

$$\sim \forall x \sim (\mathbf{Bew}(x, \mathbf{Sb}(n, 19, \mathbf{Z}(n))).$$

Wtedy może zajść jeden z dwóch następujących przypadków. Albo pewna liczba naturalna k jest numerem dowodu formuły o numerze $\mathrm{Sb}(n, 19, n)$, a więc na mocy twierdzenia istnieje w systemie dowód formuły $\mathbf{Bew}(k, \mathbf{Sb}(n, 19, n))$, albo żadna liczba naturalna nie jest numerem dowodu formuły o numerze $\mathrm{Sb}(n, 19, n)$, czyli dla każdej liczby naturalnej k istnieje dowód zdania $\sim\mathbf{Bew}(k, \mathbf{Sb}(n, 19, n))$. W pierwszym przypadku wnioskujemy od razu o sprzeczności systemu, ponieważ wynika z niego istnienie dowodu dla samej formuły g (której numerem jest przecież $\mathrm{Sb}(n, 19, n)$), mamy więc zarazem dowód formuły g oraz dowód jej zaprzeczenia, w drugim – o sprzeczności jeszcze wnioskować nie możemy, nie mamy bowiem podstaw twierdzić, że istnieje w systemie dowód zdania przeciwnego do zdania $\sim \forall x \sim (\mathbf{Bew}(x, \mathbf{Sb}(n, 19, \mathbf{Z}(n)))$. Widać jednak wyraźną niespójność między tym zdaniem, reprezentującym metamatematyczne stwierdzenie, że istnieje dowód zdania g, a zdaniami postaci $\sim \mathbf{Bew}(k, \mathbf{Sb}(n, 19, n))$, mówiącymi z kolei o każdej liczbie naturalnej, że nie jest numerem dowodu zdania g. W takim przypadku mówi się, że system jest *ω-sprzeczny*, co oznacza, że istnieje w nim zarówno dowód pewnego zdania postaci $\sim \forall x \sim \phi(x)$, jak i dowód każdego ze zdań $\sim \phi(0)$, $\sim \phi(1)$, $\sim \phi(2)$ itd. Gdy taka sytuacja nie ma miejsca, mówimy że system jest ω-niesprzeczny.

Doszliśmy zatem do twierdzenia następującej treści:

Twierdzenie Gödla o niezupełności arytmetyki. Istnieje zdanie g w języku arytmetyki PA, takie że

1. jeśli system PA jest niesprzeczny, to nie istnieje w nim dowód zdania g,
2. jeśli system PA jest ω-niesprzeczny, to nie istnieje w nim dowód zdania $\sim g$.

Tak więc system arytmetyki Peano PA jest obarczony pewną inherentną wadą. Jaką? Tego twierdzenie nie rozstrzyga: system PA jest albo co najmniej ω-sprzeczny, albo niezupełny.

W 1936 roku Barkley Rosser wzmocnił twierdzenie Gödla, usuwając założenie o ω-niesprzeczności dzięki innej konstrukcji dowodu. W ulepszonej wersji twierdzenie Gödla (i Rossera) wygląda więc następująco:

Twierdzenie Gödla-Rossera o niezupełności arytmetyki. Istnieje zdanie g w języku arytmetyki PA, takie że jeśli system PA jest niesprzeczny, to nie istnieje w nim ani dowód zdania g, ani dowód zdania $\sim g$.

Należy tu dodać, że wynik w pracy Kurta Gödla jest w istocie rzeczy mocniejszy, mówi bowiem nie tylko o systemie arytmetyki Peano, ale i o każdym jego rozszerzeniu, czyli o systemach powstałych przez dodanie do systemu PA nowych aksjomatów. Oznacza to (uwzględniając już poprawkę Rossera), że żaden system zawierający PA nie może być jednocześnie niesprzeczny i zupełny. Oznacza to także koniec nadziei na konstrukcję systemu aksjomatycznego, umożliwiającego udowodnienie każdego prawdziwego zdania matematycznego.

Pozostaje jeszcze kwestia niesprzeczności systemu PA, z której, jak widzieliśmy, wynika jego niezupełność. Czy system PA jest niesprzeczny? A dokładniej, czy można niesprzeczność systemu PA udowodnić wewnątrz tego systemu, w jego języku i jego środkami? I tu, niestety, nadzieje okazały się niemożliwe do spełnienia. Niesprzeczność systemu formalnego oznacza, że dla dowolnego zdania A w jego języku co najmniej jedno ze zdań A, $\sim A$ nie ma w systemie dowodu. Równoważnie, że istnieje co najmniej jedno zdanie, nie mające dowodu w systemie. Pamiętając o reprezentacji zdań metamatematycznych w języku systemu PA, nietrudno taki warunek zapisać jako zdanie arytmetyczne: $\sim \forall y \sim \forall x \sim \mathbf{Bew}(x,y)$, albo krócej, używając skrótu $\exists z\ \phi(z)$ zamiast $\sim \forall z \ \sim \phi(z)$,

$$(c) \qquad \exists y \sim \exists x \mathbf{Bew}(x,y),$$

czyli dosłownie: istnieje liczba y, z którą nie pozostaje w relacji **Bew** żadna liczba naturalna x. Można wykazać, że w systemie Gödla istnieje dowód implikacji

$$\exists y \sim \exists x \mathbf{Bew}(x,y) \Rightarrow \forall x \sim (\mathbf{Bew}(x, \mathbf{Sb}(n, 19, \mathbf{Z}(n)))).$$

Gdyby zatem istniał dowód niesprzeczności, który można byłoby odwzorować w systemie PA, czyli formalny dowód poprzednika tej implikacji, to korzystając z reguły odrywania uzyskalibyśmy twierdzenie systemu w postaci jej następnika. Ale tym następnikiem jest formuła g, która dowodu nie ma – jeśli system jest niesprzeczny! Zatem dowodu nie może mieć także zdanie c.

Czy to znaczy, że nie można w ogóle udowodnić niesprzeczności arytmetyki Peano? Nie. Pierwszy dowód niesprzeczności arytmetyki podał Gerhard Gentzen w 1936 roku, korzystał jednak w nim ze środków, których w języku arytmetyki wyrazić nie można. Inaczej mówiąc, musiał odwołać się do systemu bogatszego (teorii mnogości), by ten wynik uzyskać. I tak to już jest: aby udowodnić niesprzeczność systemu zawierającego arytmetykę, trzeba przyjąć założenie o niesprzeczności bogatszego systemu. Absolutny dowód niesprzeczności pozostaje nierealizowalnym marzeniem.

Gerhard Gentzen, *Die Widerspruchsfreiheit der reinen Zahlentheorie*, Math. Annalen 112(1936), 493–565

Kurt Gödel, *Über formal unenstcheidbare Sätze der Principia Mathematica und verwandter Systeme I*, Monatsh. Math. u. Phys. 38 (1931), 173–198

Barkley Rosser, *Extensions of some theorems of Gödel and Church*, Journ. Symb. Logic 1 (1936), N1, 87–91

oraz

Ernest Nagel, James R. Newman, *Twierdzenie Gödla*, PWN, Warszawa 1966 (tłum. B. Stanosz)