Czy Wielkie Twierdzenie Fermata jest ważnym zagadnieniem matematycznym?

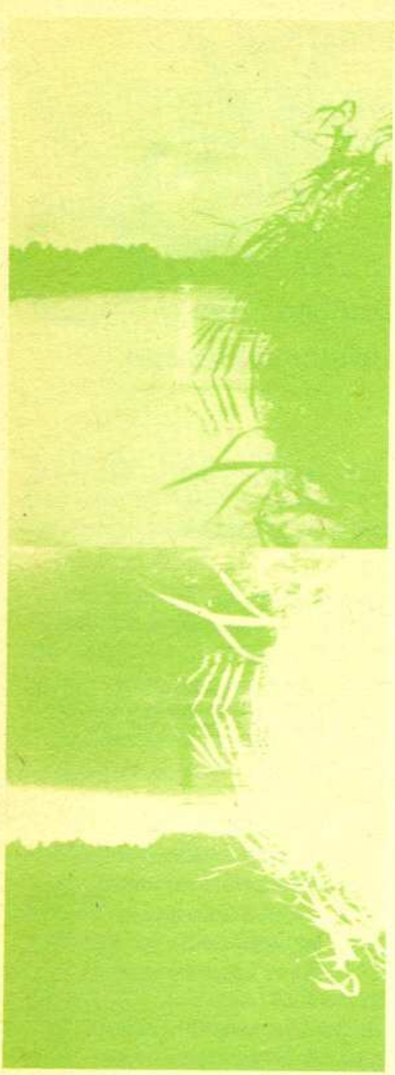
Rozmowa z *profesorem dr. Andrzejem SCHINZLEM*, członkiem korespondentem Polskiej Akademii Nauk, wiceprezesem Polskiego Towarzystwa Matematycznego

— Panie Profesorze, często w matematyce słyszymy opinię: to jest ważne twierdzenie. Czy można wytłumaczyć, jakie kryteria przyjmujemy uznając odkrycie (czy hipotezę) za ważne? W teorii liczb granica między ważnym twierdzeniem a efektownym jednostkowym faktem wydaje mi się dość wąska...

— Rozróżniłbym dwa dosyć pokrewne pojęcia: twierdzenie *ważne* i *poważne*. Przytoczę może kilka myśli matematyka angielskiego Hardy'ego. W swojej książce „*A Mathematician's Apology*" pisze on, że jego zdaniem powaga (*seriousness*) twierdzenia nie leży w jego konsekwencjach, ale w znaczeniu idei matematycznych, które wiąże. Idea matematyczna jest *znacząca*, jeżeli, z grubsza mówiąc, może być w naturalny i konkretny sposób związana z szerokim kompleksem innych idei. Szekspir wywarł ogromny wpływ na rozwój języka angielskiego, Otway prawie żadnego, ale to nie dlatego Szekspir był lepszym poetą. Był lepszym poetą po prostu dlatego, że pisał lepsze wiersze.
Znaczenie idei matematycznych można mierzyć ich *ogólnością* i *głębokością*. Hardy pisze, że żadnej z tych jakości nie umie określić precyzyjnie, ale ogólność idei matematycznej polega na jej istotnej obecności w wielu konstrukcjach, w dowodach wielu twierdzeń różnorodnych typów. Na przykład dowód Pitagorasa niewymierności liczby $\sqrt{2}$ dopuszcza wiele daleko idących uogólnień. Zwykle łatwiej jednak zobaczyć, że twierdzenie *nie jest* poważne: gdy mianowicie dotyczy tylko izolowanych, kuriozalnych osobliwości. Na przykład: że 8712 i 9801 są jedynymi liczbami czterocyfrowymi, podzielnymi przez swoje „odwrotności": 2178 i 1089. Albo że 1, 153, 370, 371 i 407 są jedynymi liczbami równymi sumie sześcianów swoich cyfr. Ogólności twierdzenia — pisze dalej Hardy — nie należy rozumieć w sensie logicznym, tzn. że dotyczy ono bytów abstrakcyjnych, a nie „konkretnych". Pewna umiarkowana generalizacja musi być obecna w każdej myśli matematycznej, ale każda rzecz jest właśnie tą rzeczą, a nie czym innym. Różnice między rzeczami są co najmniej tak samo interesujące jak podobieństwa. Nie wybieramy przecież swoich przyjaciół dlatego, że ucieleśniają oni wszystkie miłe cechy ludzkości, ale dlatego, że są właśnie tacy, jacy są. Własność wspólna zbyt wielu obiektom rzadko może być naprawdę interesująca. Tu Hardy z kolei cytuje Whiteheada: „owocna koncepcja polega na połączeniu poważnych uogólnień z ograniczeniami narzuconymi przez szczegółowość", *happy particularity*, jak pisze Whitehead w „*Science and the Modern World*".

Nieco dwuznacznie brzmiące po angielsku zdanie ujmuje to tak: General embedded in the concrete ... G. Pólya powiedział: matematyk, który umie tylko uogólniać, przypomina małpę, która umie tylko wchodzić po drzewach; a ten kto umie tylko stosować twierdzenia — małpę, która umie tylko schodzić z drzew...,

— Hardy pisze dalej o głębokości twierdzeń i pojęć matematycznych. Ma to pewien związek z trudnościami: na ogół im głębsza myśl, tym trudniej ją pojąć do końca. Nie jest to jednak reguła: idee zawarte w dowodzie Pitagorasa niewymierności $\sqrt{2}$ są bardzo głębokie, ale nikt nie uzna ich dziś za trudne. Idee matematyczne są jednak ułożone — pisze dalej Hardy — warstwowo. Każda warstwa, każde piętro jest pełne wzajemnych połączeń z pojęciami leżącymi wyżej, niżej i na tym samym poziomie. Im niższe piętro, im głębsza warstwa, tym głębsze (i na ogół tym trudniejsze) pojęcie. I tak na przykład „niewymierność" jest czymś głębszym niż pojęcie liczby całkowitej, a twierdzenie Pitagorasa o niewymierności $\sqrt{2}$ głębsze niż twierdzenie Euklidesa o tym, że liczb pierwszych jest nieskończenie wiele.
Tyle, jeśli chodzi o książkę Hardy'ego, z której wybrałem, moim zdaniem, najciekawsze fragmenty. Chciałbym dorzucić jeszcze kilka swoich uwag. Jak już wspomniałem, oprócz pojęcia powagi można, przynajmniej w teorii liczb, mówić o ważności twierdzeń. Tak nazwałbym te twierdzenia, które niosą w sobie wiele informacji o liczbach naturalnych. Teoria liczb jest w tej specyficznej sytuacji, że ma pewien jasno określony przedmiot badań; można go porównać do przedmiotu badań biologii. To jest inaczej, zupełnie inaczej, niż, powiedzmy, w algebrze.
I wobec tego są w teorii liczb twierdzenia zawierające *wiele informacji* nie będące *poważnymi* w sensie Hardy'ego.



— Wspomniał Pan o „biologicznym" charakterze teorii liczb. Jako koronny przykład prostego, ale trudnego zagadnienia bywa najczęściej wymieniany problem Fermata nazywany przeważnie Wielkim Twierdzeniem Fermata: równanie $x^n+y^n = z^n$ nie ma rozwiązań naturalnych, gdy $n > 2$. Czy rozstrzygnięcie tego zagadnienia stałoby się punktem zwrotnym teorii liczb, jej kamieniem milowym, czy stałoby się jej świętem?

— Byłoby na pewno świętem dla teoretyków liczb, bo pozbyliby się może zmory amatorów nadsyłających „dowody" Wielkiego Twierdzenia Fermata. Natomiast nie byłoby ani punktem zwrotnym, ani kamieniem milowym. Wielkie Twierdzenie Fermata stanowi doskonały przykład twierdzenia, które jest *poważne* w sensie Hardy'ego, ale które nie jest *ważne* w sensie, który właśnie podałem. Niewątpliwie, rozwiązanie tego zagadnienia wiąże się z bardzo licznymi ideami teorii liczb, zresztą nawet całej matematyki. Do Wielkiego Twierdzenia Fermata Kummer stworzył teorię „czynników idealnych", którą potem sformalizował Dedekind i z której powstała bardzo dziś ważna w algebrze teoria ideałów. Dlatego jest to poważne zagadnienie. Nie jest za to, według mnie, *ważne*. Sądzę — a poparłaby mnie na pewno większość matematyków — że informacja, jakiej o liczbach naturalnych dostarcza nam to twierdzenie, jest stosunkowo skąpa. Porównam to może z innym sławnym zagadnieniem teorii liczb: *zagadnieniem Goldbacha* (czy każda liczba parzysta większa od 2 jest sumą dwóch liczb pierwszych). To zagadnienie jest otwarte od 240 lat, ale postępy w jego rozwiązaniu mają inny charakter niż te przy twierdzeniu Fermata. Dotychczasowe wysiłki przynoszące znaczny postęp w hipotezie Goldbacha doprowadzały od razu do całej serii podobnych wyników uzyskiwanych tą samą metodą. Na przykład dowód Winogradowa, że każda dostatecznie duża liczba nieparzysta jest sumą trzech liczb pierwszych (a więc każda dostatecznie duża parzysta — sumą czterech; wystarczy odjąć 3) przenosi się na przypadek kombinacji liniowej liczb pierwszych ze współczynnikami całkowitymi. Natomiast przy Wielkim Twierdzeniu Fermata może się okazać, że równanie $x^n+y^n = z^n$ żadnych rozwiązań w liczbach naturalnych nie ma, ale już dla równania $x^n+y^n = 2z^n$ tą metodą nie da się otrzymać „oczekiwanego" wyniku ($x = y = z$). Tu właśnie tkwi różnica, dosyć wyraźna, między Wielkim Twierdzeniem Fermata a hipotezą Goldbacha. W tym ostatnim zagadnieniu każdy postęp przynosi całą serię nowych rezultatów, a w zagadnieniu Fermata każdy postęp w metodach byłby bardzo ważny, ale obecnie otrzymuje się wyniki tylko bardzo specjalne. Gdybym miał więc klasyfikować hipotezy teorii liczb z punktu widzenia ważności, a nie ich powagi, to na pierwszym miejscu postawiłbym uogólnioną hipotezę Riemanna o zerach szeregów Dirichleta. Ma ona najwięcej różnorodnych, już wyprowadzonych z niej konsekwencji: o rozmieszczeniu liczb pierwszych albo np. o najmniejszej nie-reszcie kwadratowej. Jest to sławny problem w teorii liczb: dla danej liczby pierwszej p oszacować od góry jej najmniejszą nie-resztę kwadratową. Uogólniona hipoteza Riemanna daje natychmiast oszacowanie przez $(\ln p)^2$. Stanowczo ta właśnie hipoteza teorii liczb prowadzi do największej liczby rozstrzygających wyników.

— A propos twierdzenia Fermata. Jest ono dziś udowodnione dla wykładników $n \leqslant 125\,000$ (Wagstaff, 1978). Wiadomo zaś, że ewentualne pierwiastki równania Fermata muszą być większe niż wykładnik, tzn. co najmniej 125 000. To chyba zupełnie niweczy szanse znalezienia kontrprzykładu metodami „usiąść przy biurku — albo przy komputerze — i wyliczyć"?

— Tak, to oczywiste. Z tym że oszacowanie przez wykładnik, o którym Pan wspomniał, jest dość trywialne. Bardziej dokładne jest następujące: jeżeli $x^p+y^p = z^p$ (x, y, z — naturalne, p — liczba pierwsza > 2; zagadnienie Fermata wystarczy badać dla wykładników będących liczbami pierwszymi), to x, y i z są równe co najmniej p^p. Można znaleźć zresztą i precyzyjniejsze oszacowanie (np. K. Inkeri w 1953 r.).

— No tak, zatem żeby wyrachować, że konkretne x, y, z są rozwiązaniem, musielibyśmy działać na liczbach większych niż $125\,000^{15625000000}$, mających zatem ponad 80 miliardów cyfr. To wciąż za duże liczby dla maszyn cyfrowych.
Wspomniał Pan też o tym, że rozwiązanie problemu Fermata przerwałoby może falę listów z jego „dowodami", jakie wciąż przysyłają amatorzy. Nb. „Delta" też dostawała. Jednak z powodu swojego „biologicznego" charakteru teoria liczb jest specyficzną dyscypliną matematyczną. Większość bowiem gałęzi matematyki jest niezrozumiała dla laika. Żeby ją zrozumieć, trzeba włożyć dużo wysiłku. Dlatego zresztą tak trudno popularyzować matematykę nie spłaszczając jej. Tymczasem duże liczby każdy sobie jakoś tam wyobraża; każdemu można wytłumaczyć, co to jest liczba pierwsza i „pokazać" największą znaną. Zwrot „rozłożyć na czynniki pierwsze" wszedł nawet do języka potocznego. Wielu ludzi szuka rozwiązania równania Fermata posługując się kalkulatorami elektronicznymi. Czy można jeszcze coś odkryć w teorii liczb nie będąc profesjonalistą?

— Nieprofesjonalistą matematykiem czy nie — matematykiem?

— Nie — matematykiem.

— Mogę przytoczyć bardzo ciekawy przykład. W 1978 roku emerytowany urzędnik bankowy H. L. S. Orde opublikował w „*Journal of the London Mathematical Society*" elementarny dowód

Mówimy, że liczba naturalna a jest nie-resztą kwadratową modulo p (gdzie p jest liczbą pierwszą), gdy kongruencja

$$x^2 \equiv a \pmod{p}$$

nie ma rozwiązania w liczbach całkowitych.

wzoru Dirichleta dla liczby klas ciał kwadratowych o ujemnym wyróżniku. Było to otwarte zagadnienie od ponad 100 lat. Znane dowody tego twierdzenia wykorzystywały metody analityczne, nieelementarne, związane z przejściem granicznym. Dowód elementarny próbowało bezskutecznie znaleźć wielu matematyków, a największy sukces odniósł w 1927 roku matematyk radziecki Wienkow, który podał dowód obejmujący większość — ale nie wszystkie — możliwe wyróżniki. Panu H. L. S. Orde udało się podać dowód kompletny. Sprawdza się więc powiedzenie „wszyscy wiedzieli, że to się nie da zrobić; ignorant nie wiedział i zrobił". A więc jest jeszcze pole do popisu dla amatorów w teorii liczb, chociaż rzecz jest niewątpliwie bardzo trudna. Przede wszystkim jest olbrzymia możliwość, że jeżeli „amator" nawet znajdzie jakiś cenny wynik, to ktoś to już odkrył przed nim. Przecież teorią liczb zajmuje się tak wielu ludzi od tak dawna. Bez dokładnego zbadania literatury można dojść do dawno znanych rzeczy. Tak właśnie się zdarzyło na konkursie prac maturalnych PTM i „Delty" w 1982 roku. Jeden z uczniów uogólnił pewne twierdzenie zawarte w książce Sierpińskiego o teorii liczb, ale nie orientował się, że w międzyczasie otrzymano już rezultat znacznie ogólniejszy. Muszę jednocześnie dodać, że rok przedtem w podobnym konkursie pan Jarosław Wróblewski uzyskał w swojej pracy maturalnej ciekawy i zupełnie nowy wynik.

— *Kolejne moje pytanie jest związane z poprzednim. Załóżmy, że młody człowiek (uczeń albo student) interesuje się teorią liczb i chciałby się nią zajmować. Czego powinien się nauczyć? Czy teoria liczb jest samowystarczalną dyscypliną matematyki (jak np. niektóre działy geometrii), czy, przeciwnie, korzysta z twierdzeń innych dyscyplin matematycznych?*

Teoria liczb korzysta w wysokim stopniu z twierdzeń innych dyscyplin. Można powiedzieć, że wyzyskuje te dziedziny, bo bierze od nich więcej, niż sama im daje. A czego się trzeba nauczyć, chcąc specjalizować się w teorii liczb? To bardzo zależy od działu samej teorii liczb. Nie ma już na świecie osób, które zajmowałyby się wszystkimi czy nawet większością jej działów. Do badań np. nad rozmieszczeniem liczb pierwszych niezbędne są wiadomości z teorii funkcji analitycznych. Do algebraicznej teorii liczb najbardziej potrzebna jest algebra abstrakcyjna, choć przydaje się też teoria funkcji analitycznych. W probabilistycznej teorii liczb niezbędny jest, oczywiście, rachunek prawdopodobieństwa, do równań diofantycznych geometria algebraiczna... . Nie znaczy to wcale, że najpierw trzeba opanować jakąś poboczną dziedzinę, a potem wziąć się za teorię liczb. W trakcie studiów teorioliczbowych należy po prostu pogłębiać wiadomości z odpowiednich działów matematyki.

— *Specjalizacja w teorii liczb może być skomplikowana, choćby dlatego, że rzadko w programach uniwersyteckich znajduje się wykład albo seminarium z tej dziedziny. Nie ma takiego seminarium w Uniwersytecie Warszawskim ...*

W uniwersytecie rzeczywiście, ale od 20 lat odbywa się seminarium z teorii liczb w Instytucie Matematycznym PAN. Jest ono zresztą kontynuacją poprzednio istniejącego uniwersyteckiego i trafiają na nie także studenci. W ostatnich latach miałem kilku doktorantów, którzy swoje prace magisterskie napisali przedtem na tym właśnie seminarium. To nie jest więc zupełna pustka. Wiem, że w roku 1981/82 prof. Władysław Narkiewicz z Uniwersytetu Wrocławskiego prowadził z teorii liczb wykład kursowy.

— *Warto tu chyba przypomnieć, że na Międzynarodowym Kongresie Matematyków w Helsinkach w 1978 roku jedynym Polakiem, którego zaproszono do wygłoszenia referatu sekcyjnego, był młody pracownik Instytutu Matematycznego PAN doc. Henryk Iwaniec, specjalizujący się właśnie w teorii liczb. Zaproszenie do wygłoszenia referatu na kongresie jest wielkim wyróżnieniem dla matematyka — dowodzi bowiem, że dany uczony ma rzeczywiście światową sławę w dziedzinie, którą się zajmuje. Wyższym wyróżnieniem dla matematyka jest chyba tylko referat plenarny na kongresie — no i medal Fieldsa, odpowiednik nagrody Nobla dla matematyków.*

— Tak, to prawda.

— *Dziękuję za rozmowę.*

Rozmawiał *Michał SZUREK*

Dwa dzielenia

Weźmy dwie liczby naturalne a i b, przy czym niech $b > a$. Jeżeli będziemy dla różnych liczb naturalnych k obliczali resztę z dzielenia $k \cdot (k+a)$ przez $(k+b)$, to okaże się, że prawie zawsze otrzymywać będziemy ten sam wynik.

Weźmy np. $a = 3$, $b = 5$. Mamy wówczas

$$57\,(57+3) = 55\,(57+5) \quad \text{reszta } 10,$$
$$100\,(100+3) = 98\,(100+5) \quad \text{reszta } 10,$$
$$222\,(222+3) = 220\,(222+5) \quad \text{reszta } 10$$

itd.

Dlaczego tak się dzieje? Dla tych, którzy nie umieli bądź nie mieli ochoty sprawdzić, rozwiązanie na stronie 11. Tam też można znaleźć wyjaśnienie, dlaczego ta notatka ma właśnie taki a nie inny tytuł.

dr Piotr RUDNICKI