dr hab. Mariusz Skałba,
Wydział Matematyki
Uniwersytet Warszawski
e-mail: skalba@mimuw.edu.pl

Recenzja pracy doktorskiej pani mgr Karoliny Chałupki *Pewne równania diofantyczne typu Fermata i krzywe eliptyczne*

Głównym tematem recenzowanej pracy są równania diofantyczne podobnego typu jak słynne równanie z wielkiego twierdzenia Fermata

$$x^n + y^n = z^n.$$

Jak powszechnie wiadomo nie ma uniwersalnych metod rozwiązywania równań diofantycznych - vide negatywne rozwiązanie X problemu Hilberta. Z drugiej strony matematycy wypracowali wiele skutecznych metod eksploracji konkretnych klas równań. Oprócz licznych metod ad hoc, na ogół elementarnych, poczesne miejsce zajmują:

(A) metody oparte na faktoryzacji w odpowiednio dobranym pierścieniu liczbowym i ogólniej, wykorzystujące arytmetykę w tym pierścieniu lub w odpowiednim pierścieniu lokalnym;

(B) metody oparte na teorii aproksymacji diofantycznych (zarówno archimedesowych jak i p-adycznych);

(C) metody korzystające z twierdzenia o modularności krzywych eliptycznych określonych nad $\mathbb{Q}$ i pokrewnych faktów, udowodnionych stosunkowo niedawno.

Autorka używa w swoich badaniach przede wszystkim nowoczesnych metod typu (C). Ale warto od razu zauważyć, że istotną rolę w jej metodzie odgrywają również bardziej klasyczne podejścia (A) i (B). Charakterystyczne dla równań diofantycznych typu Fermata jest to, że przez wiele dziesiątek lat były one poza zasięgiem metod (A) i (B). Dopiero powiązanie hipotetycznych rozwiązań badanych równań z krzywymi eliptycznymi i formami modularnymi pozwoliło przełamać impas: po sensacyjnym wyniku Wilesa z lat 90-tych przyszły następne ciekawe rezultaty innych matematyków.

Badania doktorantki wpisują się w rozwój metod typu (C).

U podstaw tych metod leży pomysł Freya, aby z hipotetycznym rozwiązaniem równania diofantycznego, o którym chcemy udowodnić, że nie ma rozwiązań, związać pewną krzywą eliptyczną. Następnie należy poddać ją wnikliwym badaniom po to, aby w końcu uzyskać sprzeczność. Areną tych wnikliwych badań jest redukcja równania tej krzywej mod p dla wszystkich **bez wyjątku** liczb pierwszych p. Dla typowej liczby pierwszej p, a więc takiej która nie dzieli wyróżnika krzywej zredukowana krzywa jest gładka, a więc dalej eliptyczna. Paradoksalnie ten typowy przypadek jest najmniej istotny dla omawianej metody. Istotne i subtelne zjawiska występują w przypadku, gdy liczba pierwsza p dzieli wyróżnik globalnego modelu minimalnego. Zredukowana krzywa ma wtedy punkt osobliwy. Rodzaj osobliwości jest dokładnie zakodowany w przewodniku krzywej.

Pani Chałupka obliczyła najpierw wyróżniki i przewodniki krzywych typu Freya powiązanych z badanymi równaniami. Ponadto opisała podstawowe własności i parametry reprezentacji absolutnej grupy Galois ciała $\overline{\mathbb{Q}}$ działającej na module Tate'a odpowiedniej krzywej eliptycznej oraz reprezentacji stowarzyszonej z odpowiednio dobraną formą modularną. Konfrontacja tych wszystkich informacji, wspomagana komputerowo, prowadzi do warunków, na parametry wyjściowego równania, które prowadzą do sprzeczności.

Zaletą tych wyników jest pewnego rodzaju *jednostajność* nierozwiązalności – prototypem jest tutaj oryginalne równanie Fermata i teza, że nie ma ono rozwiązań "jednostajnie"dla wszystkich $n > 2$.

I tak np. w rozdziale 2 autorka udowodniła (między innymi) następujące twierdzenie (Twierdzenie 2.1):

Jeśli C jest liczbą całkowitą podzielną przez 3 wolną od trzecich potęg oraz p jest liczbą pierwszą spełniającą $p > \mathrm{rad}(C)^{10\mathrm{rad}(C)^2}$ [1] to równanie

$$x^p + y^p = Cz^3$$

nie posiada rozwiązań pierwotnych. Rezultaty tego rozdziału zostały opublikowane w pracy [Kra1].

Dokładne opisanie rodzaju osobliwości dla liczb pierwszych $p = 2, 3$ jest technicznie skomplikowane - autorka korzysta wielokrotnie z algorytmu Tate'a oraz specjalnych wyników zawartych w tabelach pracy [Pap93].

W rozdziale 4 autorka zajmuje się równaniami typu

$$(x + y)(x^2 + Bxy + y^2) = Dz^p \tag{1}$$

gdzie $p \geq 7$ jest liczbą pierwszą, $B \in \{0, 1, 3, 4, 5, 6\}$, a $D \geq 1$ musi mieć bardziej specjalną postać. Te wyniki zostały w części opublikowane we wspólnej pracy [DJK12]. Najciekawsze i najbardziej oryginalne wyniki

[1] $\mathrm{rad}(C)$ oznacza iloczyn różnych dzielników pierwszych liczby C.

doktorantka uzyskała w rozdziałach 5 i 6, wieńczących dysertację. Omówię je dokładniej. W rozdziale 5 autorka przedstawiła pełną klasyfikację krzywych eliptycznych E określonych nad $\mathbb{Q}$ o przewodniku $N(E) \in \{16q, 48q, 64q, 128q, 192q, 384q\}$, gdzie q jest liczbą pierwszą, które mają punkt wymierny rzędu 2. Okazuje się (najkrócej rzecz ujmując), że q musi spełniać jedno z 39 równań diofantycznych z parametrami, wśród których jest zawsze q (równania (28) do (66)). Jeszcze bardziej imponujące jest zastosowanie tej klasyfikacji w rozdziale 6 do równania diofantycznego (1) dla D postaci $D = q^\alpha$, przy czym $q \notin S$. S oznacza tu zbiór tych liczb pierwszych q dla których jedno z równań (28)-(66) ma rozwiązanie. Twierdzenie 6.1 mówi, że S ma gęstość naturalną 0 w obrębie liczb pierwszych - jego dowód jest technicznie skomplikowany i różnorodny: wymaga zastosowania różnorakich metod typu (A) i (B). Natomiast Twierdzenie 6.2 mówi, że jeśli $B \in \{0, 1, 4, 6\}$, $q \notin S$, $\alpha \geq 1$, $D = q^\alpha$ oraz p jest liczbą pierwszą $p > q^{16q}$ to równanie (1) nie posiada nietrywialnego rozwiązania pierwotnego (x, y, z), gdzie $z \neq \pm 1$.

Zestawiając oba twierdzenia doktorantka otrzymuje Wniosek 6.3 w którym walor "jednostajności"jest istotny:

Niech $B \in \{0, 1, 4, 6\}$. *Dla liczby pierwszej* q *ze zbioru gęstości* 1 *w zbiorze liczb pierwszych, równanie (1) ma skończenie wiele rozwiązań* (x, y, z, α, p), *gdzie* x, y, z *są względnie pierwszymi, niezerowymi liczbami całkowitymi, zaś* α *i* $p \geq 4$ *są liczbami naturalnymi.*

Sprawne i skuteczne stosowanie różnorakich metod badania równań diofantycznych ((A), (B) i (C)) zasługuje na uznanie. Istotnym elementem pracy jest zaprzęgnięcie do obliczeń pakietu obliczeniowego Magma. Należy jednak podkreślić, że to wspomaganie komputerowe nie dałoby ciekawych rezultatów bez dobrych pomysłów formalnych, które rozsiane są po całej pracy. Doktorantka wielokrotnie wykazała się dogłębnym zrozumieniem i biegłością w stosowaniu zarówno najnowocześniejszych metod algebraicznej teorii liczb jak i jej bardziej klasycznych technik (np. aproksymacji diofantycznych).

Oczywiście jak każdy autor, doktorantka nie ustrzegła się drobnych błędów i tak np. zakresy wykładników f_2, f_3 na stronie 10 są podane błędnie. W sformułowaniu twierdzenia 6.1 status możliwego przewodnika $32q$ nie jest dla mnie jasny. Tego typu drobne uchybienia nie wpływają jednak na moją wysoką ocenę całej pracy doktorskiej. Nie mam wątpliwości, że pani Chałupka jest świetnie przygotowana do pracy badawczej w obszarze równań diofantycznych. Przedstawiona przez nią dysertacja spełnia wszystkie tradycyjne i ustawowe wymogi dotyczące prac doktorskich. Dlatego wnoszę o jej dopuszczenie do dalszych etapów przewodu doktorskiego.

Warszawa, 14.12.2019r.

M. Skałba