MATERIAŁY IX KONFERENCJI SZKOLENIOWEJ
Z TEORII ZAGADNIEŃ EKSTREMALNYCH

1987 Łódź s. 153

O WYNIKU FALTINGSA

T. Krasiński (Łódź)

0. WSTĘP. Geometria diofantyczna zajmuje się badaniem równań diofantycznych metodami geometrii algebraicznej. Młody matematyk niemiecki Gerd Faltings (rok urodzenia 1954) za wyniki z tej dziedziny otrzymał nagrodę Fieldsa w 1986 r. Rozstrzygnął on kilka hipotez, w tym znaną hipotezę Mordella z 1922 r. o rozwiązaniach wymiernych równań diofantycznych. W artykule tym przedstawimy krąg zagadnień prowadzących do tej hipotezy oraz omówimy wyżej wspomniane wyniki Faltingsa i ich proste konsekwencje.

1. RÓWNANIA DIOFANTYCZNE. Ten dział teorii liczb zajmuje się szukaniem rozwiązań całkowitych lub wymiernych równań postaci

$$F(X_1,\ldots,X_n) = 0, \tag{1}$$

gdzie $F \in \mathbb{Z}[X_1,..,X_n]$. W artykule ograniczymy się do problemu szukania rozwiązań wymiernych.

W geometrii algebraicznej pełniejsze wyniki otrzymuje się, gdy równanie (1), po ujednorodnieniu, badamy w przestrzeni rzutowej $\mathbb{C}P^n$. Wówczas problem będzie polegał na znalezieniu wśród wszystkich rozwiązań równania (1) w $\mathbb{C}P^n$ punktów o współrzędnych wymiernych (te ostatnie definiujemy jako te punkty $P \in \mathbb{C}P^n$, dla których istnieją współrzędne jednorodne wymierne). Dla uproszczenia będziemy zapisywać równania we współrzędnych niejednorodnych. W przypadku szukania rozwiązań w "nieskończoności" przechodzić będziemy do współrzędnych jednorodnych.

Rozpoczniemy od analizy najprostszych równań diofantycznych dwóch zmiennych (pierwotna hipoteza Mordella również dotyczyła wielomianów dwóch zmiennych).

1°. Niech $F \in \mathbb{Z}[X,Y]$ i $\deg F = 1$ tzn. $F(X,Y) = aX + bY + c$, $a,b,c \in \mathbb{Z}$ i $a \neq 0$ lub $b \neq 0$. Równanie $F = 0$ posiada nieskończenie wiele roz-

wiązań wymiernych, łatwych do wyznaczenia, oraz dokładnie jedno na prostej w nieskończoności, mianowicie $[b,-a,0]$ (bo ujednorodnienie F^* wielomianu F ma postać $F^*(X,Y,Z) = aX + bY + cZ$). Również łatwo wykazać, że równanie $F = 0$ posiada rozwiązanie całkowite wtedy i tylko wtedy, gdy $NWD(a,b) \mid c$. Ponadto, jeśli ten warunek jest spełniony, to równanie to posiada nieskończenie wiele rozwiązań całkowitych.

2°. Niech $F \in \mathbb{Z}[X,Y]$ i $\deg F = 2$. Wówczas mogą zajść trzy przypadki:

(i) wielomian F rozkłada się w $\mathbb{Q}[X,Y]$ na czynniki liniowe. Wówczas analiza rozwiązań równania $F = 0$ sprowadza się do punktu 1°,

(ii) wielomian F jest nierozkładalny w $\mathbb{Q}[X,Y]$, lecz jest rozkładalny w $\mathbb{C}[X,Y]$ np. wielomian $F(X,Y) = X^2 - 2Y^2$. Wówczas, jak wiadomo (zob. np. [8], §11, roz. X) istnieje skończone algebraiczne rozszerzenie k ciała $\mathbb{Q}$ takie, że wielomian F rozkłada się w $k[X,Y]$. W powyższym przykładzie wystarczy przyjąć $k = \mathbb{Q}(\sqrt{2})$, bo $X^2 - 2Y^2 = (X - \sqrt{2}Y)(X + \sqrt{2}Y)$.

Rozumowanie to można uogólnić. Mianowicie, niech $F \in \mathbb{Q}[X,Y]$ będzie wielomianem stopnia n, nierozkładalnym w $\mathbb{Q}[X,Y]$, lecz rozkładalnym w pewnym $K[X,Y]$, gdzie K jest rozszerzeniem ciała $\mathbb{Q}$. Wówczas istnieje skończone algebraiczne rozszerzenie k ciała $\mathbb{Q}$, że F jest rozkładalny w $k[X,Y]$. Wtedy możemy zapisać $F = F_1 \dots F_r$, $r \geq 2$, gdzie $F_i \in k[X,Y]$. Wybierając bazę $e_1,\dots,e_p$ w k nad $\mathbb{Q}$ (oczywiście $p = [k : \mathbb{Q}]$) mamy $F_i(X,Y) = G_1^i(X,Y)e_1 + \dots + G_p^i(X,Y)e_p$ dla pewnych $G_j^i \in \mathbb{Q}[X,Y]$. Stąd znikanie pewnego F_i w punkcie wymiernym jest równoważne znikaniu w tym punkcie wszystkich wielomianów G_j^i, $j = 1,\dots,p$ (na mocy liniowej niezależności e_j nad $\mathbb{Q}$). To samo postępowanie możemy zastosować do każdego z wielomianów G_j^i. Zatem po skończonej ilości kroków dojdziemy zawsze do równań (dokładniej układów równań) o współczynnikach wymiernych, które są nierozkładalne w każdym rozszerzeniu ciała $\mathbb{Q}$. Na mocy tego, w dalszym ciągu ograniczymy się do wielomianów o współczynnikach wymiernych, nierozkładalnych w $\mathbb{C}[X,Y]$.

Po tej ogólnej uwadze wróćmy do wielomianów stopnia drugiego. Na mocy powyższego rozpatrywany przypadek sprowadza się do układu równań liniowych o współczynnikach wymiernych,

(iii) wielomian F jest nierozkładalny w $\mathbb{C}[X,Y]$. Wtedy

a) jeśli równanie $F = 0$ posiada choć jedno rozwiązanie wymierne, to posiada ich nieskończenie wiele. Rzeczywiście, biorąc pod uwagę proste o współczynnikach kierunkowych wymiernych przechodzące przez ten punkt, łatwo sprawdza-

my, że drugim punktem przecięcia takiej prostej ze zbiorem $\{P \in \mathbb{C}P^2 : F^*(P) = 0$, F^* ujednorodnienie $F\}$ jest również punkt o współrzędnych wymiernych. Co więcej, przyporządkowanie to ustala "izomorfizm algebraiczny" zbioru punktów wymiernych równania $F^* = 0$ z $\mathbb{Q}P^1 = \mathbb{Q} \cup \{\infty\}$.

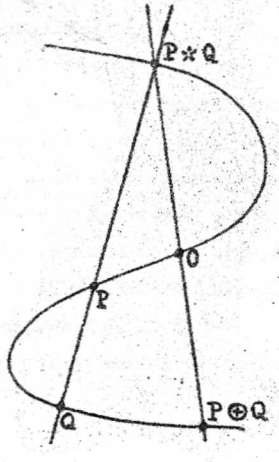
b) równanie $F = 0$ nie posiada żadnego rozwiązania wymiernego np. dla $F(X,Y) = X^2 + Y^2 + 1$.

Dla danego wielomianu nierozkładalnego w $\mathbb{C}[X,Y]$ twierdzenie Minkowskiego-Hassego (zob. [2], uwagi po tw. 1, §7, roz. 1) rozstrzyga efektywnie o tym czy zachodzi przypadek a) czy b).

3°. Niech $F \in \mathbb{Z}[X,Y]$ i $\deg F = 3$. Zgodnie z powyższym zakładamy, że wielomian F jest nierozkładalny w $\mathbb{C}[X,Y]$. Oznaczając, jak poprzednio, przez F^* ujednorodnienie F rozważmy tutaj dwa przypadki:

(i) załóżmy, że $V(F^*) = \{P \in \mathbb{C}P^2 : F^*(P) = 0\}$ jest krzywą algebraiczną nieosobliwą tzn. w żadnym punkcie $P \in V(F^*)$ nie znikają jednocześnie wszystkie pochodne cząstkowe wielomianu F^*. Jest to tzw. krzywa eliptyczna. Jako zwarta rozmaitość zespolona jednowymiarowa jest ona biholomorficznie równoważna z torusem. Te i inne wiadomości o krzywych eliptycznych można znaleźć w podręczniku [16].

Ustalmy dowolny punkt $O \in V(F^*)$. Wówczas na krzywej $V(F^*)$ możemy wprowadzić strukturę grupy abelowej za pomocą następującego działania: dla dowolnych $P,Q \in V(F^*)$ oznaczmy przez $P * Q$ trzeci punkt przecięcia prostej rzutowej przechodzącej przez P i Q z krzywą $V(F^*)$ (gdy $P = Q$ bierzemy prostą styczną). Wówczas działanie $\oplus$ w $V(F^*)$ określamy wzorem $P \oplus Q = O * (P * Q)$.



Nietrudno wykazać, że jeśli wybrany punkt 0 jest wymierny, to zbiór punktów o współrzędnych wymiernych w $V(F^*)$ tworzy podgrupę w $V(F^*)$.

Podstawowym rezultatem o strukturze tej podgrupy jest twierdzenie

TWIERDZENIE (Mordell 1922 [13]). Podgrupa punktów wymiernych krzywej eliptycznej jest skończenie generowana.

Z ogólnej teorii grup abelowych i powyższego twierdzenia wynika, że podgrupa ta jest izomorficzna z sumą prostą grup $\underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{\text{r-składników}} \oplus \mathbb{Z}/m_1\mathbb{Z} \oplus \ldots$

$\oplus\ \mathbb{Z}/m_l\mathbb{Z}$, $r \in \mathbb{N} \cup \{0\}$, $m_i \geq 2$. Liczbę r nazywamy rangą krzywej eliptycznej, zaś sumę $\mathbb{Z}/m_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/m_l\mathbb{Z}$ podgrupą torsyjną krzywej eliptycznej. Struktura tej ostatniej została zbadana przez Mazura [11]. Mianowicie, istnieje tylko 15 możliwych podgrup torsyjnych krzywych eliptycznych: 0, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}, \ldots, \mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$, $m = 2,4,6,8$. O randze wiadomo o wiele mniej. Do tej pory nie wiadomo czy istnieją krzywe eliptyczne o dowolnie dużej randze. Przykładami krzywych eliptycznych $V(F^*)$ i ich grup G punktów wymiernych są:

1° $F(X,Y) = Y^2 - X^3 - 17$, $G = \mathbb{Z} \oplus \mathbb{Z}$ generowana przez punkty $[-2,3,1]$ i $[2,5,1]$.

2° $F(X,Y) = X^3 + Y^3 - 1$, $G = \mathbb{Z}/3\mathbb{Z}$. Są to punkty $[0,1,0]$, $[1,0,0]$, $[1,-1,0] \in \mathbb{C}P^2$.

3° $F(X,Y) = 3X^3 + 4Y^3 + 5$. Równanie $F^* = 0$ nie posiada żadnego rozwiązania wymiernego w $\mathbb{C}P^2$ (zob. [3], str. 206).

(ii) Załóżmy, że krzywa $V(F^*)$ ma osobliwości (np. dla $F(X,Y) = Y^2 - X^3$ punktem osobliwym jest punkt $[0,0,1] \in \mathbb{C}P^2$). Z ogólnych twierdzeń o krzywych algebraicznych w $\mathbb{C}P^2$ wynika, że krzywa $V(F^*)$ posiada tylko jeden punkt osobliwy ([5], §4, roz. 5) i że jest dwuwymiernie równoważna $\mathbb{C}P^1$ ([5], §3, roz. 8). W tym przypadku możemy wprowadzić strukturę grupy abelowej w zbiorze punktów nieosobliwych $V(F^*)$ za pomocą analogicznego działania jak w punkcie i). Wówczas można wykazać, że podgrupa punktów o współrzędnych wymiernych jest izomorficzna bądź z grupą $\mathbb{Q}^* = \mathbb{Q} - \{0\}$ z działaniem mnożenia lub z grupą $\mathbb{Q}^+ = \mathbb{Q}$ z działaniem dodawania. Na przykład, dla wielomianu $F(X,Y) = Y^2 - X^3$ krzywa $V(F^*) = V(Y^2Z - X^3)$ ma punkt osobliwy $P = [0,0,1]$. Wówczas odwzorowanie wymierne $V(F^*) - \{P\} \ni [x,y,z] \to \frac{x}{y}$ jest izomorfizmem grupy punktów nieosobliwych $V(F^*)$ o współrzędnych wymiernych na $\mathbb{Q}^+$.

2. HIPOTEZA MORDELLA. Do chwili uzyskania przez Faltingsa wyników, o których była mowa na początku, niewiele było wiadomo o rozwiązaniach wymiernych równań $F = 0$, gdzie $F \in \mathbb{Z}[X,Y]$ i $\deg F \geq 4$. Mordell [13] w 1922 r. postawił następującą hipotezę

HIPOTEZA MORDELLA. Dla dowolnego wielomianu $F \in \mathbb{Z}[X,Y]$ nierozkładalnego w $\mathbb{C}[X,Y]$ rodzaju większego bądź równego 2, równanie $F = 0$ ma tylko skończoną ilość rozwiązań wymiernych.

Rodzaj nierozkładalnego w $\mathbb{C}[X,Y]$ wielomianu F (lub inaczej rodzaj krzywej $V(F^*)$) możemy zdefiniować na przykład na jeden z trzech równoważnych sposobów:

(i) równaniu $F = 0$ możemy jednoznacznie przyporządkować zwartą powierzchnię Riemanna. Jej rodzaj nazywamy rodzajem F.

(ii) $V(F^*)$ jest krzywą algebraiczną nieprzywiedlną (być może z osobliwościami). Po rozwiązaniu tych osobliwości (zob. np. [5], Roz. 7) otrzymamy nieosobliwą krzywą algebraiczną. Jest to jednowymiarowa rozmaitość zespolona zwarta czyli zwarta powierzchnia Riemanna. Jej rodzaj nazywamy rodzajem F.

(iii) jeśli $\deg F = n$, to rodzajem F nazywamy liczbę

$$\frac{(n-1)(n-2)}{2} - \sum_{P \in V(F^*)} \delta_P(F^*),$$

gdzie $\delta_P(F^*)$ jest pewnym liczbowym niezmiennikiem analitycznym krzywej $V(F^*)$ w punkcie P posiadającym następujące własności: $\delta_P(F^*) \geq 0$ dla każdego $P \in V(F^*)$ oraz $\delta_P(F^*) > 0$ wtedy i tylko wtedy, gdy P jest punktem osobliwym krzywej $V(F^*)$ (dokładną definicję δ_P oraz jej własności można znaleźć w [14]).

Na przykład wielomian $F(X,Y) = Y - X^{10}$ ma rodzaj 0 (punktem osobliwym krzywej $V(F^*)$ jest punkt $[0,1,0] \in \mathbb{CP}^2$). Dla $n \in \mathbb{N}$ krzywa Fermata $X^n + Y^n = Z^n$ w $\mathbb{CP}^2$ jest nieosobliwa. Zatem jej rodzaj jest równy $(n-1)(n-2)/2$. Stąd dla $n \geq 4$ krzywe Fermata mają rodzaj ≥ 2. Zauważmy, że w przypadkach rozważanych w poprzednim punkcie mamy:

1. dla $\deg F = 1$ rodzaj $F = 0$,
2. dla $\deg F = 2$ rodzaj $F = 0$,
3. dla $\deg F = 3$ rodzaj $F = 0$ lub 1 w zależności od tego czy $V(F^*)$ ma punkt osobliwy czy nie.

Powyższą hipotezę Mordella można uogólnić następująco w terminach geometrii algebraicznej

UOGÓLNIONA HIPOTEZA MORDELLA. Dowolna krzywa nierozkładalna i nieosobliwa $X \subset \mathbb{CP}^n$ określona nad ciałem liczbowym $K \supset \mathbb{Q}$, rodzaju $g \geq 2$ posiada tylko skończoną ilość punktów o współrzędnych z K.

Ciałem liczbowym nazywamy dowolne skończone algebraiczne rozszerzenie ciała liczb wymiernych, zawarte w $\mathbb{C}$, zaś zwrot "krzywa określona nad ciałem K" oznacza, że ideał tej krzywej w pierścieniu $\mathbb{C}[X_0,\ldots X_n]$ posiada generatory o współczynnikach z ciała K.

Założenie o braku osobliwości na krzywej X nie jest istotnym ograniczeniem w stosunku do klasycznej hipotezy Mordella, gdyż dla dowolnej krzywej nierozkładalnej rzutowej X określonej nad K istnieje nieosobliwa krzywa rzutowa X' określona nad K i dwuwymierne odwzorowanie $W : X' \to X$ określone również nad K (tzw. funkcje wymierne reprezentujące W mają współczynniki z K) (zob. [5], roz. 7). Za pomocą tego odwzorowania punkty o współrzędnych z K przechodzą w punkty o współrzędnych z K.

3. WYNIK FALTINGSA. Od roku postawienia hipotezy Mordella, tj. od roku 1922 do 1983, jedynymi znaczącymi rezultatami wiążącymi się z tą hipotezą były następujące dwa twierdzenia

TWIERDZENIE (Siegel 1929 [15]). Dla dowolnego ciała liczbowego $K \supset \mathbb{Q}$ i dowolnej nieosobliwej krzywej X rodzaju $g \geq 1$ określonej nad K istnieje tylko skończona ilość punktów na X o współrzędnych całkowitych (w odpowiedniej części afinicznej).

Jest rzeczą interesującą, że dowód tego twierdzenia opiera się na trudnych wynikach o aproksymacji liczb algebraicznych przez liczby wymierne (pełny dowód uogólnionej wersji twierdzenia Siegela można znaleźć w [9], roz. 8).

TWIERDZENIE (Manin 1963 [10], Grauert 1965 [6]). Uogólniona hipoteza Mordella jest prawdziwa w przypadku, gdy ciało $\mathbb{Q}$ zamienimy na ciało $K(X_1,\ldots,X_n)$ funkcji wymiernych n-zmiennych nad algebraicznie domkniętym ciałem K.

Dopiero po przeszło sześćdziesięciu latach hipoteza Mordella została rozstrzygnięta. Mianowicie, w 1983 r. G. Faltings w [4] udowodnił

TWIERDZENIE. Uogólniona hipoteza Mordella jest prawdziwa.

Bezpośrednimi wnioskami z tego twierdzenia są

WNIOSEK 1. Klasyczna hipoteza Mordella jest prawdziwa.

WNIOSEK 2. Równanie $X^n + Y^n = 1$ dla $n \geq 4$ posiada tylko skończoną ilość rozwiązań wymiernych.

Z Wniosku 2 otrzymujemy prosto następujący wynik dotyczący wielkiego twierdzenia Fermata.

WNIOSEK 3. Równanie $X^n + Y^n = Z^n$ dla $n \geq 4$ posiada co najwyżej skończoną ilość rozwiązań w liczbach całkowitych x,y,z takich, że $NWD(x,y,z) = 1$.

Na uwagę zasługuje jeszcze fakt, że Faltings w trakcie dowodu (który jest trudny i opiera się na wielu dziedzinach matematyki) wykazuje dwie inne znane hipotezy z arytmetycznej geometrii algebraicznej: Šafarevića i Tate'a. Pełny dowód rezultatów Faltingsa można również znaleźć w dodatku do rosyjskiego tłumaczenia książki [9]. Godnymi polecenia są także przeglądowe artykuły [1], [7] i [12] o tych wynikach.

SPIS LITERATURY

[1] S. Bloch, *The proof of the Mordell conjecture*, Math. Intelligencer 6 (1984), n° 2, 41-47.

[2] З. И. Боревич, И. Р. Шафаревич, *Теория чисел*, Наука, Москва, 1985.

[3] J.W.S. Cassels, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. 41 (1966), 193-291.

[4] G. Faltings, *Endlichkeitsätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), 349-366.

[5] W. Fulton, *Algebraic Curves*, The Benjamin/Cummings Publishing Company, Inc., 1978.

[6] H. Grauert, *Mordells Vermutung über Punkte auf algebraischen Kurven und Funktionenkörper*, Inst. Hautes Études Sci. Publ. Math. 25 (1965), 131-149.

[7] D. Harris, *The Mordell conjecture*, Notices Amer. Math. Soc. 33 (1986), 443-449.

[8] W.V.D. Hodge, D. Pedoe, *Methods of Algebraic Geometry, Vol.II*, Cambridge 1952.

[9] S. Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag 1983 (wyd. ros. Mir 1986).

[10] Ю.И. Манин, *Рациональные точки алгебраических кривых над функциональными полями*, Изв. АН СССР, Сер. матем. 27 (1963), 1395-1440.

[11] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. 47 (1978), 35-193.

[12] B. Mazur, *Arithmetic on curves*, Bull. Amer. Math. Soc. 14 (1986), 207-259.

[13] L. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degree*, Proc. Cambridge Philos. Soc. 21 (1923), 179--192.

[14] A. Płoski, *O niezmiennikach osobliwości krzywych analitycznych*, VII Konferencja Szkoleniowa z Teorii Zagadnień Ekstremalnych, Uniwersytet Łódzki, Łódź 1985, 80-93.

[15] C.L. Siegel, *Über einige Anwendungen Diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. Phys. Math. Kl. (1929), 41-69.

[16] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer - Verlag 1986.

Sielpia, 19-23 stycznia 1987 r.