

Ile rozwiązań ma równanie Fermata?

Magdalena Dębowska, Anna Fluder, Tomasz Szemberg

15 lutego 2007

1. Problem i jego motywacja

Jednym z największych osiągnięć teorii liczb wieńczącym minione stulecie był dowód Wielkiego Twierdzenia Fermata podany przez Wilesa [Wil]. Przypomnijmy jego wypowiedź.

Twierdzenie 1 *Niech n będzie liczbą naturalną większą bądź równą 3 i niech x, y, z będą liczbami całkowitymi takimi, że*

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

Wtedy $xyz = 0$.

Powyzsze równanie ma nieskończenie wiele rozwiązań dla wykładnika $n = 2$. Są to tak zwane trójki pitagorejskie.

Z algebraicznego punktu widzenia różnica między równaniem Pitagorasa ($n = 2$) i równaniami Fermata ($n \geq 3$) polega na tym, że opisana przez nie krzywa

$$C_n = \{(x : y : z) \in \mathbb{P}^2 : x^n + y^n - z^n = 0\}$$

jest wymierna dla $n = 2$ i ma wyższy genus dla $n \geq 3$. Twierdzenie Faltingsa [Fal] zastosowane w tej sytuacji implikuje, że na krzywej C_n dla $n \geq 4$ jest co najwyżej skończona ilość punktów o obu współrzędnych całkowitych. Nie będziemy jednak śledzić tego aspektu tutaj. Naszą uwagę skupimy na istnieniu (a raczej wyznaczeniu dokładnej ilości) rozwiązań równania Fermata w skończonej charakterystyce. Oszacowania ilości punktów dostarcza następująca nierówność Hasse-Weila:

$$\#(C_n) \leq q + 1 + 2g\sqrt{q}, \tag{1}$$

gdzie q oznacza ilość elementów ciała, a g genus krzywej.

Jak wiadomo z kursu algebry charakterystyka każdego ciała jest albo równa zero, albo jest liczbą pierwszą. Ciała o charakterystyce zero mają siłą rzeczy nieskończenie wiele elementów. Wśród ciał o skończonej charakterystyce są takie, które mają skończoną ilość

elementów. Najprostszym przykładem takiego ciała jest $\mathbb{F}_p$, które można interpretować jako zbiór liczb $\{0, 1, 2, \dots, p-1\}$ z działaniami mnożenia i dodawania indukowanymi z $\mathbb{Z}$ modulo p . Jeśli $\mathbb{F}_q$, dla pewnego $q = p^r$, jest ciałem skończonym, to można je utożsamiać z ciałem powstałym z pierścienia wielomianów $\mathbb{F}_p[X]$ przez wydzielenie pewnego ideału maksymalnego generowanego przez nierozkładalny wielomian stopnia r postaci

$$f(X) = X^r + a_1 X^{r-1} + \dots + a_r,$$

gdzie $a_1, \dots, a_r \in \mathbb{F}_p$. Ta interpretacja daje możliwość prowadzenia konkretnych obliczeń.

Rozszerzenie $\mathbb{F}_q : \mathbb{F}_p$ jest skończone, a zatem algebraiczne. Ponadto $\mathbb{F}_q$ jest ciałem rozkładu wielomianu $X^q - X$. Wynika stąd, że każde rozszerzenie postaci $\mathbb{F}_{q^k} : \mathbb{F}_q$ jest rozszerzeniem Galois. Grupa Galois tego rozszerzenia $\text{Gal}(\mathbb{F}_{q^k}/\mathbb{F}_q)$ jest cykliczna, generowana przez endomorfizm Frobeniusa

$$\varphi = \varphi_{q^k} : \mathbb{F}_{q^k} \ni \alpha \longrightarrow \alpha^q \in \mathbb{F}_{q^k}.$$

Uwaga 2 *Twierdzenie Fermata nie może być prawdziwe w skończonej charakterystyce. Wynika to z tożsamości*

$$(x + y)^p = x^p + y^p,$$

która jest prawdziwa w każdym ciele o charakterystyce równej p . (Wielu studentów uważa, że tożsamość ta zachodzi także w charakterystyce zero. Zbadanie źródeł tego przekonania pozostawiamy jednak dydaktykom.)

Przykład 3 W dowolnym ciele $\mathbb{F}_{3^k}$ zachodzi równość

$$1^3 + 1^3 = 2^3.$$

W skończonej charakterystyce zatem właściwe jest pytanie nie tyle o istnienie rozwiązań równania Fermata, ile o wyznaczenie ich dokładnej liczby. Jest to również pytanie fascynujące, szczególnie, gdy liczbę tą chce się wyznaczyć efektywnie w rozsądnym czasie.

Problem. *Wyznaczyć efektywnie ilość rozwiązań równania*

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

w (skończonym) ciele $\mathbb{F}_q$.

Problemu tego nie rozwiążemy tu w całości. Zaprezentujemy jednak dwa przypadki, które zawierają w sobie ciekawe aspekty teoretyczne.

Zacniemy od przypomnienia definicji dwóch ważnych homomorfizmów związanych z rozszerzeniami ciał.

Definicja 4 *Addytywny homomorfizm*

$$\text{Tr} = \text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q} : \mathbb{F}_{q^k} \ni \alpha \longrightarrow \alpha + \alpha^q + \dots + \alpha^{q^{k-1}} \in \mathbb{F}_q$$

nazywamy śladem.

Obraz śladu leży w $\mathbb{F}_q$, gdyż jest niezmienniczy ze względu na działanie grupy Galois rozszerzenia.

Definicja 5 *Multiplikatywny homomorfizm*

$$\text{Norm} = \text{Norm}_{\mathbb{F}_{q^k}/\mathbb{F}_q} : \mathbb{F}_{q^k} \ni \alpha \longrightarrow \alpha \cdot \alpha^q \cdot \dots \cdot \alpha^{q^{k-1}} \in \mathbb{F}_q$$

nazywamy normą.

Norma jest dobrze zdefiniowana z tych samych względów, co ślad.

2. Krzywa hermitowska

W pierwszym przykładzie rozważymy Problem dla $n = q + 1$ nad ciałem $\mathbb{F}_{q^2}$. To wygląda na bardzo szczególny przypadek. I tak jest rzeczywiście. Pozwala on jednak na zilustrowanie niezwykle użytecznego sposobu podejścia w sytuacji, która nie jest obciążona nadmiernymi komplikacjami technicznymi.

Wygodnie jest zacząć nasze rozważania od liniowej zmiany zmiennych.

$$\begin{cases} x' &= x + y \\ y' &= x + z \\ z' &= x + y + z \end{cases}$$

Równanie Fermata przyjmuje w nowych zmiennych (primy pomijamy) postać:

$$yz^q + y^qz = x^{q+1}.$$

Krzywa zadana tym równaniem jest nazywana hermitowską [RuSt]. Jest ona najlepiej znanym przykładem krzywej, która jest maksymalna tzn. ma największą możliwą z punktu widzenia oszacowania (1) ilość punktów, o czym przekonamy się za moment.

Dla $z = 0$ mamy ewidentnie dokładnie jeden punkt (w nieskończoności), który je spełnia: $(0 : 1 : 0)$. Możemy zatem ograniczyć się do części afinicznej. Podstawiając $z = 1$ dostajemy równanie

$$y + y^q = x \cdot x^q.$$

Zauważmy, że lewa strona to $\text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(y)$, zaś prawa strona to $\text{Norm}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(x)$. Niech $w \in \mathbb{F}_q^*$ będzie różnym od zera elementem. Wtedy istnieje dokładnie $\frac{q^2}{q} = q$ elementów y takich, że $\text{Tr}(y) = w$ oraz $\frac{q^2-1}{q-1} = q+1$ takich elementów x , że $\text{Norm}(x) = w$. To daje $(q-1) \cdot q \cdot (q+1)$ rozwiązań. Dodatkowe q rozwiązań otrzymujemy dla $x = w = 0$. Razem jest ich zatem q^3 , a po uwzględnieniu punktu w nieskończoności mamy $q^3 + 1$ punktów na krzywej C_{q+1} nad ciałem $\mathbb{F}_{q^2}$. Zauważmy, że w tej sytuacji genus jest równy $g(C_{q+1}) = \frac{q(q-1)}{2}$ i mamy równość w nierówności (1) (q należy zastąpić przez q^2).

3. Charakterystyka 2

W tym przykładzie podamy wzór na ilość punktów $\#X(\mathbb{F}_{2^k})$ na krzywej eliptycznej

$$X = C_3 : x^3 + y^3 = z^3$$

nad dowolnym skończonym ciałem $\mathbb{F}_{2^k}$ charakterystyki 2.

Twierdzenie 6 *Niech X będzie krzywą eliptyczną daną równaniem $x^3 + y^3 = z^3$. Wówczas ilość punktów tej krzywej nad ciałem $\mathbb{F}_{2^k}$ wyraża się wzorem*

$$\#X(\mathbb{F}_{2^k}) = \begin{cases} 2^k + 1 & \text{jeśli } k \text{ jest nieparzyste} \\ 2^k + 1 - 2(-2)^{k/2} & \text{jeśli } k \text{ jest parzyste} \end{cases}$$

Twierdzenie dotyczy nieskończonego ciągu liczb naturalnych. W teorii liczb własności ciągów często bada się za pomocą funkcji tworzących. To podejście stanowi motywację następującej, ogólnej definicji.

Definicja 7 *Niech X będzie rzutowym podzbiorem algebraicznym określonym nad ciałem $\mathbb{F}_q$ i niech $a_k := \#X(\mathbb{F}_{q^k})$. Funkcję*

$$Z_X(t) := \exp \left(\sum_{k=1}^{\infty} a_k \cdot \frac{t^k}{k} \right)$$

nazywamy funkcją zeta zbioru X (nad $\mathbb{F}_q$).

Wprost z definicji wynika tylko, że $Z_X(t)$ jest szeregiem formalnym o współczynnikach wymiernych. W istocie jest to funkcja wymierna nad $\mathbb{Q}$. To stwierdzenie stanowi treść hipotezy Weila sformułowanej około roku 1949 [Wei] i udowodnionej w 1959 przez Dworka [Dwo].

Nasza wiedza o postaci funkcji zeta jest, przynajmniej w odniesieniu do zbiorów gładkich, znacznie dokładniejsza. Wyraża to następujące twierdzenie wykazane przez Deligne [Del] i Grothendiecka [Gro].

Twierdzenie 8 *Niech X będzie gładkim zbiorem algebraicznym wymiaru d . Wówczas*

$$Z_X(t) = \frac{P_1(t) \cdots P_{2d-1}(t)}{P_0(t) \cdots P_{2d}(t)},$$

gdzie P_i są wielomianami o współczynnikach całkowitych, ze współczynnikiem wiodącym równym 1. Ich stopień jest określony przez topologię rozmaitości X , a dokładniej odpowiada i -tej liczbie Bettiego X traktowanego jako rozmaitość zespolona, $\deg P_i = \dim_{\mathbb{R}} H^i(X(\mathbb{C}), \mathbb{R})$.

Ponadto wiadomo, że wielomiany P_i są postaci

$$P_i(t) = \prod_{j=1}^{\deg P_i} (1 - \alpha_{ij}t),$$

dla pewnych liczb zespolonych α_{ij} , których moduł jest równy $|\alpha_{ij}| = q^{i/2}$ (ten fakt znany jest jako hipoteza Riemann dla rozmaitości nad ciałami skończonymi i został wykazany dla krzywych w 1948 roku przez Weila [Wei], a ogólnie w 1974 roku przez Deligne'go [Del]).

Zastosujemy teraz powyższe fakty do krzywej C_3 . Krzywa ta jest gładka i eliptyczna. Dostajemy stąd natychmiast, że

$$P_0(t) = 1 - t, \quad P_2(t) = 1 - 2t, \quad P_1(t) = (1 - \alpha t)(1 - \bar{\alpha}t)$$

dla pewnej liczby zespolonej α takiej, że $|\alpha| = \sqrt{2}$.

Powyższa postać wielomianów P_i jest prawdziwa dla dowolnej krzywej eliptycznej określonej nad ciałem $\mathbb{F}_2$. Wyliczenie α wymaga konkretnego równania. Nie jest to dziwne, gdyż ilość punktów na krzywych eliptycznych nad ciałami skończonymi nie jest stała. Z rozważań we wcześniejszym przypadku wiemy, że nad $\mathbb{F}_{2^2}$ na krzywej C_3 jest 9 punktów. Ta informacja wystarczy by wyliczyć α . Wprost z porównania postaci funkcji zeta z definicji 7 i twierdzenia 8 wynika bowiem, że

$$\#C_3(\mathbb{F}_{2^k}) = 1^k + 2^k - \alpha^k - \bar{\alpha}^k. \quad (2)$$

Zatem w szczególności

$$\#C_3(\mathbb{F}_4) = 9 = 1 + 4 - (\alpha^2 + \bar{\alpha}^2)$$

z czego wnioskujemy $\alpha = \sqrt{2}i$. W połączeniu z (2) kończy to dowód twierdzenia 6.

Literatura

- [Del] Deligne, P.: La conjecture de Weil. I. Inst. Hautes tudes Sci. Publ. Math. No. 43 (1974), 273–307
- [Dwo] Dwork, B.: On the rationality of the zeta function of an algebraic variety. Amer. J. Math. 82 (1960), 631–648
- [Fal] Faltings, G.: Endlichkeitsstze für abelsche Varietäten über Zahlkörpern. Invent. Math. 73 (1983), 349–366
- [Gro] Grothendieck, A.: Standard conjectures on algebraic cycles. 1969 Algebraic Geometry (Internat. Colloq., Tata Inst. Fund. Res., Bombay, 1968) pp. 193–199 Oxford Univ. Press, London
- [RuSt] Rück, H.G., Stichtenoth, H.: A characterization of Hermitian function fields over finite fields. J. reine angew. Math. 457 (1994), 185–188

- [Wei] Weil, A.: Numbers of solutions of equations in finite fields. Bull. Amer. Math. Soc. 55, (1949), 497–508
- [Wil] Wiles, A.: Modular elliptic curves and Fermat’s last theorem. Ann. of Math. 141 (1995), 443–551

Instytut Matematyki
Akademia Pedagogiczna
ul. Podchorążych 2
30-084 Kraków