Twierdzenie Chevalleya–Warninga i grafy p-regularne

Jakub WITASZEK[*]

Rozwiązywanie równań diofantycznych jest jednym z ważniejszych problemów klasycznej teorii liczb. Czytelnicy tego artykułu na pewno słyszeli o równaniu Pella $x^2 - dy^2 = 0$ czy równaniu Fermata $x^n + y^n = z^n$. Znane wszystkim Małe Twierdzenie Fermata mówi o rozwiązaniach $x^{p-1} - 1 \equiv 0 \pmod p$, a teoria reszt kwadratowych o $x^2 - d \equiv 0 \pmod p$. Teoria liczb jest nie tylko piękną sztuką, ale także łączy się z innymi działami nauki, między innymi z kryptografią, topologią czy geometrią algebraiczną. W tym artykule chciałbym zaprezentować przykład zastosowania równań diofantycznych w teorii grafów.

Musimy zacząć od ustalenia kilku ważnych oznaczeń. Jak zwykle $\mathbb{Z}$ to zbiór liczb całkowitych. Przez $\mathbb{Z}_p$ oznaczać będziemy zbiór wszystkich reszt z dzielenia przez p, a przez $\mathbb{Z}[x_1, x_2, \ldots, x_m]$ zbiór wielomianów o zmiennych $x_1, \ldots, x_m$ i o współczynnikach całkowitych.

Rozwiązanie zadania M 1380. Zauważmy, że

$$\begin{aligned} a^n + b^n &= ((a+b)-b)^n + b^n = \\ &= \sum_{k=1}^{n} \binom{n}{k} (a+b)^k (-b)^{n-k} + \\ &\quad + (-b)^n + b^n = \\ &= \sum_{k=1}^{n} \binom{n}{k} (a+b)^k (-b)^{n-k}, \end{aligned}$$

ponieważ $(-b)^n + b^n = 0$ dla nieparzystych n. Zatem $a^n + b^n$ przy dzieleniu przez $(a+b)^2$ daje taką samą resztę jak składnik odpowiadający $k = 1$, który wynosi $n(a+b)b^{n-1}$. Zatem $a^n + b^n$ jest podzielne przez $(a+b)^2$ wtedy i tylko wtedy, gdy nb^{n-1} jest podzielne przez $a + b$. Ponieważ a i b są względnie pierwsze, względnie pierwsze są również $a + b$ i b. Stąd otrzymujemy tezę.

Mówimy, że n-tka liczb całkowitych $(a_1, a_2, \ldots a_n)$ jest rozwiązaniem modulo p wielomianu $f \in \mathbb{Z}[x_1, \ldots, x_n]$, jeżeli $f(a_1, \ldots, a_n) \equiv 0 \pmod p$. Na przykład, para $(1, 4)$ jest rozwiązaniem modulo 5 wielomianu $x^2 + 6y$.

Rozwiązanie $(a_1, \ldots, a_n)$ modulo p nazywamy istotnym, jeśli jego współrzędne są liczbami z przedziału od 0 do $p - 1$ (czyli $a_i \in \mathbb{Z}_p$ dla $1 \leqslant i \leqslant n$). W powyższym przykładzie rozwiązanie $(1, 4)$ jest istotne, zaś $(1, 9)$ już nie. Z własności kongruencji wiemy, że jeżeli $(a_1, \ldots, a_n)$ jest rozwiązaniem, to $(a_1 \bmod p, \ldots, a_n \bmod p)$ jest rozwiązaniem istotnym. Ponadto, żeby znaleźć wszystkie rozwiązania modulo p danego równania, wystarczy znać rozwiązania istotne.

Stopniem jednomianu nazywamy sumę wykładników jego czynników, czyli, na przykład, xy^2z ma stopień 4. Stopniem wielomianu f (oznaczamy go $\deg(f)$) nazywamy najwyższy spośród stopni jego jednomianów; wobec tego dla $f(x, y, z) = xyz + 2zy^4 + 6xz^3$ mamy $\deg(f) = 5$.

Będziemy wykorzystywać następującą nieoczywistą zależność (której dowód Czytelnik Wnikliwy z pewnością spróbuje znaleźć sam):

$$(1) \qquad \sum_{x \in \mathbb{Z}_p} x^i = 1^i + 2^i + 3^i + \ldots + (p-1)^i \equiv 0 \pmod p \qquad \text{dla } 0 < i < p - 1.$$

Teraz możemy już zaprezentować tytułowe twierdzenie.

Twierdzenie Chevalleya–Warninga. *Niech $f_1, f_2, \ldots, f_m \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$ będą niezerowymi wielomianami wielu zmiennych o sumie stopni mniejszej niż liczba wszystkich zmiennych, tzn.* $\deg(f_1) + \deg(f_2) + \ldots + \deg(f_m) < n$. *Wtedy liczba ich wspólnych istotnych rozwiązań modulo p jest podzielna przez p.*

Zanim zobaczymy dowód twierdzenia, warto przyjrzeć się kilku przykładom i wnioskom. Twierdzenie Chevalleya–Warninga jest ważnym narzędziem w badaniu rozwiązalności równań diofantycznych.

Rozpatrzmy, na przykład, równanie $x^2 - 3y^2 + 7z \equiv 0 \pmod p$. Jego stopień jest równy dwa, a są trzy zmienne. Zatem z powyższego twierdzenia liczba rozwiązań istotnych jest podzielna przez p. Ten wielomian ma trywialne rozwiązanie $0^2 - 3 \cdot 0^2 + 7 \cdot 0 = 0$ i $p > 1$, więc musi istnieć także pewne rozwiązanie nietrywialne, tzn. takie, które ma przynajmniej jedną współrzędną niezerową. Na przykład, dla $p = 2$ mamy następujące cztery rozwiązania istotne: $(0, 0, 0)$, $(1, 1, 0)$, $(1, 0, 1)$ i $(0, 1, 1)$.

Odwrotnością liczby a modulo p (gdzie p jest pierwsza) nazywamy taką liczbę b, że

$$ab \equiv 1 \pmod p.$$

Rozumując podobnie, udowodnimy teraz, że równanie $a^2 + b^2 + 1 \equiv 0 \pmod p$ ma rozwiązanie. W tym celu przyjrzyjmy się równaniu $x^2 + y^2 + z^2 \equiv 0 \pmod p$. Tak samo jak w poprzednim przykładzie możemy uzasadnić, że istnieje nietrywialne rozwiązanie (x_0, y_0, z_0) modulo p. Załóżmy bez straty ogólności, że $z_0 \not\equiv 0 \pmod p$. Wtedy $p \mid (x_0 z_0^{-1})^2 + (y_0 z_0^{-1})^2 + 1$ (gdzie z_0^{-1} jest odwrotnością z_0 modulo p). A stąd wnioskujemy, że równanie $a^2 + b^2 + 1 \equiv 0 \pmod p$ ma rozwiązanie.

Dowód istnienia rozwiązania równania

$$a^2 + b^2 + 1 \equiv 0 \pmod p$$

bez użycia twierdzenia Chevalleya–Warninga jest bardzo ciekawym zadaniem, zachęcam Czytelników do zastanowienia się nad nim!

Zwróćmy jeszcze uwagę na pewną delikatną kwestię mogącą wzbudzać niepokój. Weźmy, na przykład, równanie $x^2 + y^2 \equiv 0 \pmod 3$. Ma ono dokładnie jedno istotne rozwiązanie – trywialne. Liczba zmiennych jest równa stopniowi wielomianu, więc nie możemy stosować twierdzenia Chevalleya–Warninga. Ale $x^2 + y^2 + 0 \cdot z \equiv 0 \pmod 3$, równoważne naszemu, ma już trzy zmienne i stopień równy 2. Czy zatem otrzymaliśmy sprzeczność w matematyce? Nie: zmieniła nam się liczba zmiennych i zbiór rozwiązań jest już trójelementowy: $(0, 0, 0)$, $(0, 0, 1)$, $(0, 0, 2)$.

[*]student, Universität Bonn

Rozwiązanie zadania M 1379.
Niech K będzie najmniejszą liczbą o tej własności, że $f(x) \leqslant K$ dla każdej liczby rzeczywistej x. Pokażemy, że wówczas f jest funkcją stałą, równą K w każdym punkcie. Załóżmy nie wprost, że dla pewnego z jest $f(z) < K$. Skoro

$$\frac{f(z)+K}{2} < K,$$

to z określenia liczby K znajdziemy liczbę x, dla której

$$\frac{f(z)+K}{2} < f(x).$$

To jednak daje sprzeczność, bowiem

$$\frac{f(z)+K}{2} < f(x) = f\left(\frac{z+2x-z}{2}\right) \leqslant$$
$$\leqslant \frac{f(z)+f(2x-z)}{2} \leqslant \frac{f(z)+K}{2}.$$

Przejdźmy do dowodu twierdzenia. Główny pomysł to wyrażenie liczby wspólnych rozwiązań w postaci ładnej funkcji – najlepiej także wielomianu.

Wykażemy najpierw, że wielomian

$$W(x_1,\ldots,x_n) = \\ = (1-f_1(x_1,\ldots,x_n)^{p-1})(1-f_2(x_1,\ldots,x_n)^{p-1})\ldots(1-f_m(x_1,\ldots,x_n)^{p-1})$$

przystaje do 1 modulo p, jeżeli $(x_1,\ldots,x_n)$ jest wspólnym rozwiązaniem $f_1, f_2, \ldots, f_n$, i przystaje do 0 w przeciwnym przypadku. Dlaczego tak jest? Z Małego Twierdzenia Fermata $a^{p-1} \equiv 0$ lub 1 modulo p w zależności od tego, czy p dzieli a, czy nie. Zatem i-ty czynnik W przystaje do 1 dla rozwiązania f_i modulo p, a do 0 w przeciwnej sytuacji.

Wynika stąd, że liczba istotnych rozwiązań przystaje modulo p do

$$\sum_{x_1,x_2,\ldots,x_n\in\mathbb{Z}_p} W(x_1,\ldots,x_n).$$

Musimy udowodnić, że ta suma jest podzielna przez p.

Niech $H(x_1,x_2,\ldots,x_n) = x_1^{a_1}x_2^{a_2}\ldots x_n^{a_n}$ będzie pewnym jednomianem W. Wykażemy najpierw, że

$$p \,\Big|\, \sum_{x_1,x_2,\ldots,x_n\in\mathbb{Z}_p} H(x_1,\ldots,x_n). \tag{2}$$

Zauważmy, że

$$\sum_{x_1,x_2,\ldots,x_n\in\mathbb{Z}_p} H(x_1,x_2,\ldots,x_n) = \sum_{x_1,x_2,\ldots,x_n\in\mathbb{Z}_p} x_1^{a_1}x_2^{a_2}\ldots x_n^{a_n} = \\ = \Big(\sum_{x_1\in\mathbb{Z}_p} x_1^{a_1}\Big)\Big(\sum_{x_2\in\mathbb{Z}_p} x_2^{a_2}\Big)\ldots\Big(\sum_{x_n\in\mathbb{Z}_p} x_n^{a_n}\Big).$$

Suma wszystkich wykładników a_i jest mniejsza niż $(p-1)n$, gdyż

$$a_1+a_2+\ldots+a_n = \deg(H) \leqslant \deg(W) = (p-1)(\deg(f_1)+\ldots+\deg(f_m)) < (p-1)n$$

(ostatnia nierówność wynika z założeń twierdzenia). Dlatego istnieje przynajmniej jeden wykładnik a_k mniejszy niż $p-1$. Dla $a_k = 0$ wzór (2) jest prawdziwy, ponieważ k-ty czynnik w powyższym iloczynie jest równy p. Natomiast dla $a_k > 0$ ze wzoru (1) otrzymujemy

$$\sum_{x_k\in\mathbb{Z}_p} x_k^{a_k} = 1^{a_k} + 2^{a_k} + \ldots + (p-1)^{a_k} \equiv 0 \pmod p,$$

zatem także i cały iloczyn jest podzielny przez p.

Ponieważ W jest sumą swoich jednomianów, to również

$$p \,\Big|\, \sum_{x_1,x_2,\ldots,x_n\in\mathbb{Z}_p} W(x_1,\ldots,x_n),$$

co należało wykazać. □

Użyjemy teraz twierdzenia Chevalleya–Warninga do rozwiązania problemu z teorii grafów. Stopniem wierzchołka grafu będziemy nazywali liczbę krawędzi z niego wychodzących. Zakładamy, że graf nie ma pętelek (krawędzi o tym samym początku i końcu). Mówimy, że graf jest n-regularny, jeżeli stopień każdego wierzchołka jest równy n. Badanie takich grafów pasjonowało wielu matematyków, szczególnie że – ze względu na swoją symetrię – naturalnie pojawiają się one w licznych problemach. Ciągle istnieje wiele nierozwiązanych hipotez dotyczących tej klasy grafów.

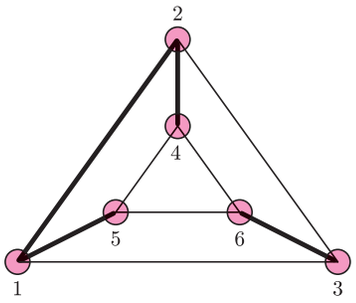
Twierdzenie o podgrafie p-regularnym. *Niech G będzie grafem $2p-1$ regularnym dla pewnej liczby pierwszej p. Wtedy w G istnieje spójny p-regularny podgraf.*

Idea dowodu polega na opisaniu świata kombinatorycznego równaniami diofantycznymi. Niech E będzie zbiorem krawędzi, a V zbiorem wierzchołków G. Niech H będzie (niekoniecznie spójnym) podgrafem G zawierającym wszystkie jego wierzchołki (jak na rysunku). Krawędzi w G o końcach i,j przypiszmy pewną niezerową liczbę $x_{i,j} \in \mathbb{Z}_p$, jeżeli ta krawędź leży w H, i zero w przeciwnym przypadku. Stopień i-tego wierzchołka w H (oznaczany dalej $\deg(i,H)$) przystaje modulo p, na mocy Małego Twierdzenia Fermata, do

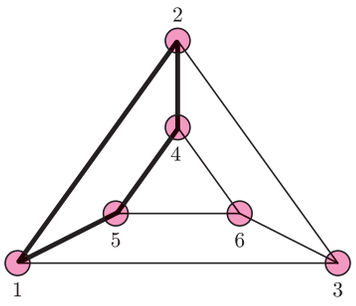
$$\sum_{v\in V,\,(i,v)\in E} x_{i,v}^{p-1}$$

I odwrotnie, zauważmy, że każdy wybór liczb $x_{i,j} \in \mathbb{Z}_p$ daje nam pewien podgraf H (zakładamy, że zawiera on wszystkie wierzchołki G). Kluczowe w dowodzie jest

Spójrzmy na przykłady opisanego w artykule przyporządkowania. Pogrubione krawędzie należą go podgrafu H.



W tym przykładzie mamy $x_{1,5} \neq 0$, $x_{1,2} \neq 0$, $x_{2,4} \neq 0$ oraz $x_{3,6} \neq 0$. Podgraf H składa się z dwóch składowych. Mamy też, między innymi, $\deg(1,H) = 2$, a $\deg(5,H) = 1$.



Tym razem $x_{1,5} \neq 0$, $x_{1,2} \neq 0$, $x_{2,4} \neq 0$ oraz $x_{4,5} \neq 0$. Podgraf H składa się z trzech składowych – jednego podgrafu 2-regularnego i dwóch podgrafów trywialnych (wierzchołków izolowanych). Ponadto $\deg(1, H) = 2$ i $\deg(5, H) = 2$.

spostrzeżenie, że wystarczy znaleźć nietrywialny podgraf H (lub równoważnie liczby $x_{i,j} \in \mathbb{Z}_p$, nie wszystkie zerowe), którego każdy wierzchołek ma stopień podzielny przez p (czyli $p \mid \deg(i, H)$). Dlaczego? Nietrywialny podgraf H ma nietrywialną spójną składową. Nietrywialna spójna składowa takiego H będzie właśnie szukanym p-podgrafem: $p \mid \deg(i, H)$ i $\deg(i, H) \leqslant 2p - 1$, więc $\deg(i, H)$ jest równy 0 lub p, ale w tej nietrywialnej spójnej składowej każdy wierzchołek będzie miał stopień p, bo wierzchołki stopnia 0 są izolowane.

Udało nam się sprowadzić nasz problem do rozwiązania układu równań diofantycznych

$$\deg(i, H) \equiv \sum_{v \in G,\, (i,v) \in E} x_{i,v}^{p-1} \equiv 0 \pmod{p}.$$

Tych wielomianów jest $|G|$, każdy ma stopień $p - 1$ i zależy od zmiennych $x_{i,j}$ (dla wszystkich i, j połączonych krawędzią w G). Suma stopni tych wielomianów jest równa $(p - 1)|G|$. Liczba zmiennych jest taka sama jak liczba krawędzi w G, czyli $\frac{1}{2}(2p - 1)|G|$ (każdy wierzchołek G ma stopień $2p - 1$ i każda krawędź ma dwa końce) – to więcej niż $(p - 1)|G|$. Ponieważ ten układ równań diofantycznych ma trywialne rozwiązanie oraz $p > 1$, więc z twierdzenia Chevalleya–Warninga istnieje szukane rozwiązanie nietrywialne.

Powyższe twierdzenie zostało także udowodnione dla p będącego potęgą liczby pierwszej, ale do tej pory nie wiadomo, czy jest ono prawdziwe dla dowolnej liczby naturalnej. Łącząc otrzymany przez nas rezultat z argumentami kombinatorycznymi, można wykazać, że dla $k \geqslant 4r$ każdy k-regularny graf bez pętelek zawiera podgraf r-regularny.

Czytelników zainteresowanych tematem zachęcam do zajrzenia do pracy Nogi Alona *Combinatorial Nullstellensatz*, która była moją inspiracją do napisania tego artykułu. Praca ta została wydrukowana w 8. numerze czasopisma *Combinatorics, Probability and Computing*, jest też dostępna na stronie internetowej autora. Można w niej znaleźć dowody różnych twierdzeń kombinatorycznych i tych dotyczących addytywnej teorii liczb.

Warto jeszcze zwrócić uwagę, że nie przypadkiem udało nam się opisać zagadnienie kombinatoryczne za pomocą układu równań diofantycznych. Można udowodnić metatwierdzenie, że każdy skończony problem kombinatoryczny (np. dotyczący grafów) można sprowadzić do rozwiązania pewnego równania diofantycznego modulo p (formalnie, każdy podzbiór w $\mathbb{Z}_p^n$ jest zbiorem zer pewnego wielomianu). Niestety, rozwiązanie takiego równania diofantycznego jest prawie zawsze dużo trudniejsze niż rozwiązanie zagadnienia, od którego wyszliśmy.

Zdegenerowany trójkąt

Sensacyjna (i słaba naukowo) powieść Dana Browna *Anioły i demony* rozpoczyna się wątkiem zamordowania Leonarda Vetry, księdza i fizyka, którego celem było naukę „doprowadzić do tego, by potwierdzała istnienie Boga” oraz „udowodnienie, że zdarzenia opisane w Księdze Rodzaju były możliwe”. W swej najnowszej książce pt. *Filozofia przypadku* Michał Heller, także ksiądz i fizyk, jawi się jako przeciwieństwo tej postaci.

Chociaż podstawowym tematem książki jest, jak wskazuje tytuł, pojęcie przypadku, na drugim planie czai się pytanie, które od lat jest przyczyną gorących debat. Skąd się bierze ewolucja od prostszych do bardziej skomplikowanych struktur (biologiczna lub kosmiczna) i jak interpretować prawa nią rządzące?

Michał Heller wskazuje we wstępie do *Filozofii przypadku* na krańce mapy możliwych opinii w tej kwestii. Przywołuje nazwiska Richarda Dawkinsa, wybitnego propagatora teorii ewolucji, dla którego występujący w jej sformułowaniu czynnik przypadkowości w pewnym momencie zaczął stanowić argument na rzecz radykalnego ateizmu, oraz Williama Dembskiego, jednego z twórców tzw. inteligentnego projektu, czyli koncepcji, że w przyrodzie można znaleźć gdzieniegdzie nieredukowalną złożoność, świadczącą o ingerencji Stwórcy w proces kształtowania się życia. Choć Heller tego nie czyni w systematyczny sposób, ciekawe jest poszukać na tej mapie stanowisk wyrażanych przez kościoły. Na przykład, w dokumentach polskiego Episkopatu znajdujemy opinię, iż „pewne środowiska ateistyczne usiłują zastępować chrześcijańską naukę o stworzeniu ideologicznym, materialistycznym ewolucjonizmem [...] od głoszenia »przypadku« jako źródła wszystkiego, co istnieje, przez przyjęcie »ślepych sił natury« [...] jako wyłącznych sił sprawczych w procesach ewolucyjnych” (stanowisko Rady Naukowej Konferencji Episkopatu Polski, 2006).

We wszystkich wzmiankowanych stanowiskach słowo „przypadek” jest wyraźnie przeciwstawione czynnikom racjonalnym, determinizmowi, czy zgoła planowemu działaniu. *Filozofia przypadku* poświęcona jest przede wszystkim „odczarowaniu” tego słowa. Obecność powyższego rozumienia przypadku w filozofii i teologii jest, zdaniem Hellera, niechlubną spuścizną po Arystotelesie, ignorującą powstanie i rozwój rachunku prawdopodobieństwa oraz teorii układów dynamicznych jako dojrzałych i ważnych gałęzi matematyki. By nie być gołosłownym, historii tych dziedzin wiedzy autor przypatruje się uważnie przez sporą część książki. Ta podróż przez wieki i idee przygotowuje czytelnika na tezę wyrażoną w ostatniej części książki: z punktu widzenia fizyka układy podlegające ewolucji (obserwowalna część Wszechświata, organizm żywy) należy modelować jako otwarte, nieliniowe układy dynamiczne (być może nawet deterministyczne!), których stan może się niekiedy znacznie zmieniać w wyniku oddziaływania z fluktuacją środowiska.

Dla Hellera możliwość wyrażenia i studiowania praw przyrody w języku matematyki i fizyki wskazuje na istnienie Wielkiej Kosmicznej Matrycy realizującej to, co Einstein nazwał Zamysłem Boga. Jeśliby jednak odrzucić niewymagane przez przyrodę interpretacje, okaże się, że poglądy Hellera lokują się bardzo blisko analogicznie odfiltrowanych poglądów Dawkinsa. Skromnie wydana, lecz ciekawie udokumentowana i niezwykle wciągająca książka okazuje się zatem aktem nieomal wywrotowym.

K. T.

M. Heller, *Filozofia przypadku*, Copernicus Center Press, Kraków 2012.