Jak rozwiązać równanie diofantyczne o skończonej liczbie rozwiązań całkowitych?

Apoloniusz TYSZKA, Kraków

Równanie diofantyczne to równanie postaci $D(x_1, \ldots, x_p) = 0$, gdzie $D(x_1, \ldots, x_p)$ jest wielomianem o współczynnikach całkowitych. Negatywne rozwiązanie 10. problemu Hilberta mówi, że nie istnieje algorytm rozstrzygający, czy równanie diofantyczne ma jakieś rozwiązanie całkowite. Udowodnił to Yuri Matiyasevich w 1970 roku, patrz [1], [2], [5], [8] i [9]. Nie istnieje też algorytm rozstrzygający, czy liczba rozwiązań całkowitych równania diofantycznego jest skończona czy nieskończona, patrz [6] i [8] str. 129–130.

Pytanie z tytułu dotyczy istnienia algorytmu, który przyjmuje na wejściu wielomian $D(x_1, \ldots, x_p)$ o współczynnikach całkowitych i zwraca skończony ciąg całkowitych p-tek, którego wyrazy tworzą zbiór wszystkich całkowitych rozwiązań równania $D(x_1, \ldots, x_p) = 0$, jeżeli jest on skończony. Równoważne pytanie brzmi: *Czy istnieje algorytm, który każdemu równaniu diofantycznemu przyporządkowuje liczbę naturalną większą od modułów rozwiązań całkowitych, gdy rozwiązania te tworzą zbiór skończony?*

Yu. Matiyasevich przypuszcza, że taki algorytm nie istnieje, patrz [9] str. 42. Inne przypuszczenie mówi, że poszukiwany algorytm istnieje dla równań z dwiema zmiennymi, patrz [18] str. 247. Dla równań z jedną zmienną konstrukcja takiego algorytmu wynika z istnienia obliczalnego górnego ograniczenia modułów pierwiastków rzeczywistych wielomianu o współczynnikach całkowitych. W artykule przedstawimy przypuszczenie, które prowadzi do konstrukcji poszukiwanego algorytmu.

Niech E_n oznacza układ równań

$$\{x_i = 1,\ x_i + x_j = x_k,\ x_i \cdot x_j = x_k :\ i, j, k \in \{1, \ldots, n\}\}.$$

Twierdzenie. *Gdy wielomian $D(x_1, \ldots, x_p)$ o współczynnikach całkowitych ma niezerowy stopień względem każdej zmiennej x_i, to równanie $D(x_1, \ldots, x_p) = 0$ można przedstawić równoważnie jako układ $S \subseteq E_n$, gdzie*

$$n = (2M + 1)^{(d_1 + 1) \cdot \ldots \cdot (d_p + 1)},$$

M oznacza maksimum modułów współczynników wielomianu $D(x_1, \ldots, x_p)$ i dla każdego $i \in \{1, \ldots, p\}$ d_i jest stopniem wielomianu $D(x_1, \ldots, x_p)$ względem zmiennej x_i.

Dowód. Rozważmy zbiór T wszystkich wielomianów $W(x_1, \ldots, x_p)$ o współczynnikach całkowitych z przedziału $[-M, M]$, dla których dla każdego $i \in \{1, \ldots, p\}$ stopień wielomianu $W(x_1, \ldots, x_p)$ względem zmiennej x_i nie przekracza stopnia wielomianu $D(x_1, \ldots, x_p)$ względem zmiennej x_i. Niech $\mathrm{card}(T)$ oznacza liczebność zbioru T. Wówczas

$$\mathrm{card}(T) = (2M + 1)^{(d_1 + 1) \cdot \ldots \cdot (d_p + 1)}$$

Każdemu wielomianowi należącemu do $T \setminus \{x_1, \ldots, x_p\}$ przypiszmy nową zmienną x_i, gdzie $i \in \{p + 1, \ldots, \mathrm{card}(T)\}$. Wówczas $D(x_1, \ldots, x_p) = x_q$ dla dokładnie jednego $q \in \{1, \ldots, \mathrm{card}(T)\}$. Niech H oznacza zbiór tych równań należących do $E_{\mathrm{card}(T)}$, które są tożsamościami w T. Układ równań

$$S = H \cup \{x_q + x_q = x_q\} \subseteq E_{\mathrm{card}(T)}$$

równoważnie wyraża równość $D(x_1, \ldots, x_p) = 0$ i ma tyle samo rozwiązań całkowitych, co równanie $D(x_1, \ldots, x_p) = 0$. □

W pracach [12] i [16] przedstawiamy bardziej szczegółowy dowód. Dla równania $x_1 \cdot x_2 = 1$ algorytm z powyższego dowodu wyznacza układ zawierający $(2 \cdot 1 + 1)^{(1+1) \cdot (1+1)} = 81$ zmiennych i składający się z jednego równania postaci $x_i = 1$, 2402 równań postaci $x_i + x_j = x_k$ i 549 równań postaci $x_i \cdot x_j = x_k$, patrz [16].

Thoralf Skolem udowodnił, że każde równanie diofantyczne może być algorytmicznie przekształcone na równoważny układ równań diofantycznych stopnia co najwyżej drugiego, patrz [10, str. 2–3], [3, str. 386–387, dowód Theorem 1], [5, str. 262–263, dowód Theorem 7.5] i [8, str. 3–4]. Np. równanie $x_1^5 - x_1 = x_2^2 - x_2$ jest równoważne poniższemu układowi *(U)*:

$$(U)\ \begin{cases} x_1 \cdot x_1 = x_3 \\ x_3 \cdot x_3 = x_4 \\ x_1 \cdot x_4 = x_5 \\ x_1 + x_6 = x_5 \\ x_2 \cdot x_2 = x_7 \\ x_2 + x_6 = x_7 \end{cases}$$

Układ *(U)* jest mały, bo został znaleziony *ad hoc*. Gdy układ równoważny zdefiniujemy tak, jak w dowodzie Twierdzenia, będzie on zawierał $(2 \cdot 1 + 1)^{(2+1) \cdot (5+1)} = 3^{18}$ zmiennych.

Dla wielu równań diofantycznych o skończoności zbioru rozwiązań całkowitych wiemy z twierdzeń, których dowody nie dostarczają obliczalnego ograniczenia modułów rozwiązań. Twierdzenie wraz z poniższym przypuszczeniem implikuje, że pomijając ogrom obliczeń można znaleźć wszystkie rozwiązania tych równań diofantycznych, dla których liczba rozwiązań jest skończona.

Przypuszczenie 1. *Jeśli tylko skończenie wiele całkowitych n-tek $(x_1, \ldots, x_n)$ rozwiązuje układ $S \subseteq E_n$, to każde takie $(x_1, \ldots, x_n)$ spełnia* $|x_1|, \ldots, |x_n| \leqslant 2^{2^{n-1}}$.

Przypuszczenie 1 zostało potwierdzone dla $n \in \{1, 2, 3\}$, patrz [12]. Dla $n \geqslant 2$ ograniczenie $2^{2^{n-1}}$ nie może być zmniejszone, bo układ

$$\begin{cases} x_1 + x_1 = x_2 \\ x_1 \cdot x_1 = x_2 \\ x_2 \cdot x_2 = x_3 \\ x_3 \cdot x_3 = x_4 \\ \ldots \\ x_{n-1} \cdot x_{n-1} = x_n \end{cases}$$

ma dokładnie dwa rozwiązania całkowite, a mianowicie $(0, \ldots, 0)$ i $\left(2, 4, 16, 256, \ldots, 2^{2^{n-2}}, 2^{2^{n-1}}\right)$.

Każdemu układowi $S \subseteq E_n$ przyporządkujemy układ $\widetilde{S}$ zdefiniowany jako

$$(S \setminus \{x_i = 1 : \ i \in \{1, \ldots, n\}\}) \cup$$
$$\{x_i \cdot x_j = x_j : \ i, j \in \{1, \ldots, n\} \text{ i równanie } x_i = 1 \text{ należy do } S\}$$

Innymi słowy, aby otrzymać $\widetilde{S}$ usuwamy z S każde równanie $x_i = 1$ i zastępujemy je przez następujące n równań:

$$x_i \cdot x_1 = x_1$$
$$\ldots$$
$$x_i \cdot x_n = x_n$$

Lemat. *Dla każdego układu $S \subseteq E_n$*

$$\{(x_1, \ldots, x_n) \in \mathbb{Z}^n : \ (x_1, \ldots, x_n) \text{ rozwiązuje } \widetilde{S}\} =$$
$$\{(x_1, \ldots, x_n) \in \mathbb{Z}^n : \ (x_1, \ldots, x_n) \text{ rozwiązuje } S\} \cup \{(0, \ldots, 0)\}$$

Lemat implikuje równoważność Przypuszczeń 1–3.

Przypuszczenie 2. *Jeśli tylko skończenie wiele całkowitych n-tek $(x_1, \ldots, x_n)$ rozwiązuje układ $S \subseteq \{x_i + x_j = x_k, \ x_i \cdot x_j = x_k : \ i, j, k \in \{1, \ldots, n\}\}$, to każde takie $(x_1, \ldots, x_n)$ spełnia* $|x_1|, \ldots, |x_n| \leqslant 2^{2^{n-1}}$.

Przypuszczenie 3. *Dla każdej całkowitej n-tki $(x_1, \ldots, x_n)$, jeśli* $2^{2^{n-1}} < \max(|x_1|, \ldots, |x_n|)$, *to istnieje całkowita n-tka $(y_1, \ldots, y_n)$, dla której* $\max(|x_1|, \ldots, |x_n|) < \max(|y_1|, \ldots, |y_n|)$ *i dla każdych i, j, k od 1 do n $x_i + x_j = x_k$ implikuje $y_i + y_j = y_k$ i dla każdych i, j, k od 1 do n $x_i \cdot x_j = x_k$ implikuje $y_i \cdot y_j = y_k$.*

Przestawiając liczbę z maksymalnym modułem na początek n-tki $(x_1, \ldots, x_n)$ otrzymujemy, że zdanie

$$\forall x_1, \ldots, x_n \in \mathbb{Z} \ \exists y_1, \ldots, y_n \in \mathbb{Z}$$
$$\left(2^{2^{n-1}} < |x_1| \Longrightarrow (|x_1| < |y_1| \vee \ldots \vee |x_1| < |y_n|)\right) \wedge$$
$$\left(\forall i, j, k \in \{1, \ldots, n\} \ (x_i + x_j = x_k \Longrightarrow y_i + y_j = y_k)\right) \wedge$$
$$\left(\forall i, j, k \in \{1, \ldots, n\} \ (x_i \cdot x_j = x_k \Longrightarrow y_i \cdot y_j = y_k)\right)$$

jest równoważne Przypuszczeniu 3. Przypuszczenie w tej postaci wyraża hipotetyczną własność arytmetyki liczb całkowitych.

Wszystkimi rozwiązaniami całkowitymi równania $x_1^5 - x_1 = x_2^2 - x_2$ są pary $(-1, 0)$, $(-1, 1)$, $(0, 0)$, $(0, 1)$, $(1, 0)$, $(1, 1)$, $(2, -5)$, $(2, 6)$, $(3, -15)$, $(3, 16)$, $(30, -4929)$ i $(30, 4930)$, patrz [4]. Wykażemy, że rozwiązania te można obliczyć korzystając z Przypuszczenia 1 i założenia, że równanie ma tylko skończenie wiele rozwiązań całkowitych. Równanie jest równoważne poniższemu układowi *(U)*:

$$(U) \begin{cases} x_1 \cdot x_1 = x_3 \\ x_3 \cdot x_3 = x_4 \\ x_1 \cdot x_4 = x_5 \\ x_1 + x_6 = x_5 \\ x_2 \cdot x_2 = x_7 \\ x_2 + x_6 = x_7 \end{cases}$$

Każda liczba rzeczywista x_2 spełnia nierówność $x_2^2 - x_2 \geqslant -\frac{1}{4}$, więc w dziedzinie liczb całkowitych równość $x_1^5 - x_1 = x_2^2 - x_2$ implikuje $-1 \leqslant x_1$. Stosując Przypuszczenie 1 otrzymujemy, że każde całkowite rozwiązanie układu *(U)* spełnia $|x_1^5| = |x_5| \leqslant 2^{2^{7-1}} = 2^{64}$. Zatem, $-1 \leqslant x_1 \leqslant \left[2^{\frac{64}{5}}\right] = 7131$, gdzie $[\cdot]$ oznacza część całkowitą. W tym zakresie zmiennej całkowitej x_1 równoważne równanie diofantyczne $4x_1^5 - 4x_1 + 1 = (2x_2 - 1)^2$ zostało rozwiązane komputerowo, patrz [14]. Rozwiązania te są identyczne z już przedstawionymi.

Obserwacja 1. *Dla wszystkich dodatnich całkowitych n, m spełniających $n \leqslant m$, jeżeli Przypuszczenie 3 jest fałszywe dla pewnej całkowitej n-tki $(x_1, \ldots, x_n)$ i $2^{2^{m-1}} < |x_1| \leqslant 2^{2^m}$, to jest ono także fałszywe dla m-tki $(\underbrace{x_1, \ldots, x_1}_{m-n+1 \text{ razy}}, x_2, \ldots, x_n)$. Analogiczne stwierdzenie jest prawdziwe dla dowolnego indeksu $k \in \{1, \ldots, n\}$.*

Na mocy Obserwacji 1, Przypuszczenie 3 rozważane łącznie dla wszystkich n jest równoważne Przypuszczeniu 4 rozważanemu łącznie dla wszystkich n.

Przypuszczenie 4. *Dla każdej całkowitej n-tki $(x_1, \ldots, x_n)$, jeśli $2^{2^{n-1}} < \max(|x_1|, \ldots, |x_n|) \leqslant 2^{2^n}$, to istnieje całkowita n-tka $(y_1, \ldots, y_n)$, dla której $\max(|x_1|, \ldots, |x_n|) < \max(|y_1|, \ldots, |y_n|)$ i dla każdych i, j, k od 1 do n $x_i + x_j = x_k$ implikuje $y_i + y_j = y_k$ i dla każdych i, j, k od 1 do n $x_i \cdot x_j = x_k$ implikuje $y_i \cdot y_j = y_k$.*

Obserwacja 2. *Jeżeli $k \in \{1, \ldots, n\}$ i całkowita n-tka $(x_1, \ldots, x_n)$ spełnia $2^{2^{n-1}} < \max(|x_1|, \ldots, |x_n|) = |x_k| \leqslant 2^{2^n}$, to fałszywość Przypuszczenia 4 dla $(x_1, \ldots, x_n)$ implikuje, że jest ono fałszywe także dla $(x_1, \ldots, x_n, x_k^2)$. Ten ciąg $n+1$ liczb całkowitych spełnia warunek $2^{2^n} < \max(|x_1|, \ldots, |x_n|, |x_k^2|) = |x_k|^2 \leqslant 2^{2^{n+1}}$.*

Dla ustalonego n, Przypuszczenie 4 może zostać potwierdzone (lecz nie obalone) przez sprawdzenie skończenie wielu całkowitych n-tek $(x_1, \ldots, x_n)$. Na mocy Obserwacji 2, jeśli Przypuszczenie 4 jest fałszywe dla jakiegoś n, to jest też fałszywe dla $n+1, n+2, n+3, \ldots$. Można więc napisać program, który wykonuje nieskończenie wiele kroków i kolejno wypisuje wszystkie liczby naturalne $n \geqslant 2$, dla których Przypuszczenie 4 jest prawdziwe, patrz [7], [15] i [17]. Jeżeli Przypuszczenie 4 jest fałszywe, to wyjście programu jest skończone i na końcu jest całkowita n-tka $(a_1, \ldots, a_n)$, gdzie $n \geqslant 4$, $2^{2^{n-1}} < \max\big(|a_1|, \ldots, |a_n|\big) \leqslant 2^{2^n}$ i układ

$$\{x_i + x_j = x_k : \quad (i, j, k \in \{1, \ldots, n\}) \wedge (a_i + a_j = a_k)\} \cup$$
$$\{x_i \cdot x_j = x_k : \quad (i, j, k \in \{1, \ldots, n\}) \wedge (a_i \cdot a_j = a_k)\}$$

jest kontrprzykładem dla Przypuszczenia 2.

Zapis na wyjściu tego programu po nieskończenie wielu krokach odnosi się do spełnialności, a nie dowiedlności zdania

$$\forall n \geqslant 2 \text{ Przypuszczenie 4 dla } n\text{-tek}$$

w jakimś systemie aksjomatycznym. Niech $\mathcal{P}$ oznacza powyższe zdanie. Jest ono równoważne zdaniu

$$\forall n \geqslant 1 \text{ Przypuszczenie 1 dla podukładów układu } E_n$$

Rozważmy algorytm, który generuje wszystkie skończone ciągi formuł języka teorii mnogości *ZFC* w kolejności liczby użytych znaków i zwraca każde $\mathcal{W} \in \{\mathcal{P}, \neg\mathcal{P}\}$, gdy jest to pierwszy napotkany dowód $\mathcal{W}$ w *ZFC*.

Na wyjściu algorytmu jest $\mathcal{P}$ i $\neg\mathcal{P}$ wtedy i tylko wtedy, gdy *ZFC* jest sprzeczna.

Na wyjściu algorytmu jest dokładnie $\mathcal{P}$ wtedy i tylko wtedy, gdy $\mathcal{P}$ jest dowiedlne w *ZFC* i *ZFC* jest niesprzeczna.

Na wyjściu algorytmu jest dokładnie $\neg\mathcal{P}$ wtedy i tylko wtedy, gdy $\neg\mathcal{P}$ jest dowiedlne w *ZFC* i *ZFC* jest niesprzeczna.

Wyjście algorytmu jest puste wtedy i tylko wtedy, gdy $\mathcal{P}$ jest nierozstrzygalne w *ZFC*.

Nie jest znane doświadczenie fizyczne, którego wyniki mogą być odczytane i zinterpretowane jako rozstrzygnięcie zdania $\mathcal{P}$. Możliwość zrealizowania obliczeń wykonywanych w nieskończenie wielu krokach jest rozważana przez fizykę teoretyczną, patrz rozdział VIII *„Relativistic and Quantum Hypercomputation”* książki [11].

Literatura

[1] Z. Adamowicz, *X Problem Hilberta*, w: *Problemy Hilberta: w pięćdziesięciolecie śmierci ich twórcy* (red. W. Więsław), str. 123–128, Instytut Historii Nauki PAN, Warszawa, 1997,
http://www.cyf-kr.edu.pl/~rttyszka/Adamowicz.pdf.

[2] Z. Adamowicz, P. Zbierski, *Logika matematyczna,* PWN, Warszawa, 1991.

[3] J. L. Britton, *Integer solutions of systems of quadratic equations,* Math. Proc. Cambridge Philos. Soc. 86 (1979), nr 3, str. 385–389.

[4] Y. Bugeaud, M. Mignotte, S. Siksek, M. Stoll, Sz. Tengely, *Integral points on hyperelliptic curves,* Algebra & Number Theory 2 (2008), nr 8, str. 859–885,
http://arxiv.org/abs/0801.4459.

[5] M. Davis, *Hilbert's tenth problem is unsolvable*, Amer. Math. Monthly 80 (1973), no. 3, 233–269,
http://mathdl.maa.org/images/upload_library/22/Ford/MartinDavis.pdf.

[6] M. Davis, *On the number of solutions of Diophantine equations,* Proc. Amer. Math. Soc. 35 (1972), nr 2, str. 552–554,
http://www.jstor.org/stable/2037646.

[7] W. Kulik, *Program w Pascalu dla niekończącego się algorytmu wypisującego kolejno wszystkie liczby naturalne $n \geqslant 2$, dla których prawdziwe jest Przypuszczenie 4*,
http://www.cyf-kr.edu.pl/~rttyszka/program.pas,
http://www.cyf-kr.edu.pl/~rttyszka/program.exe.

[8] Yu. Matiyasevich, *Hilbert's tenth problem,* MIT Press, Cambridge, MA, 1993,
http://www.cyf-kr.edu.pl/~rttyszka/strony_3_4.pdf,
http://www.cyf-kr.edu.pl/~rttyszka/strony_129_130.pdf.

[9] Yu. Matiyasevich, *Hilbert's tenth problem: what was done and what is to be done.* Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), str. 1–47, Contemp. Math. 270, Amer. Math. Soc., Providence, RI, 2000,
http://www.cyf-kr.edu.pl/~rttyszka/Appendix_6.pdf.

[10] Th. Skolem, *Diophantische Gleichungen*, Julius Springer, Berlin, 1938,
http://www.cyf-kr.edu.pl/~rttyszka/strony_1_3.pdf.

[11] A. Syropoulos, *Hypercomputation: Computing beyond the Church-Turing barrier,* Springer, New York, 2008.

MuPAD to system algebry komputerowej w *MATLABie*. Programy w [14] i [15] są również wykonywalne przez darmowy *MuPAD Light*, patrz [13].

[12] A. Tyszka, *A hypothetical upper bound for the solutions of a Diophantine equation with a finite number of solutions*,
http://arxiv.org/abs/0901.2093.

[13] A. Tyszka, *Linki do pliku instalacyjnego MuPADa Light*,
http://www.cyf-kr.edu.pl/~rttyszka/MuPAD-Install.html.

[14] A. Tyszka, *Program w MuPADzie rozwiązujący równanie $x_1^5 - x_1 = x_2^2 - x_2$,*
http://www.cyf-kr.edu.pl/~rttyszka/program_i_rozwiazania.txt.

[15] A. Tyszka, *Programy w MuPADzie dla niekończącego się algorytmu wypisującego kolejno wszystkie liczby naturalne $n \geqslant 2$, dla których prawdziwe jest Przypuszczenie 4,*
http://www.cyf-kr.edu.pl/~rttyszka/program1.txt,
http://www.cyf-kr.edu.pl/~rttyszka/program1a.txt,
http://www.cyf-kr.edu.pl/~rttyszka/1000wynikow.txt.

[16] A. Tyszka, K. Molenda, M. Sporysz, *An algorithm which transforms any Diophantine equation into an equivalent system of equations of the forms $x_i = 1$, $x_i + x_j = x_k$, $x_i \cdot x_j = x_k$,* Int. Math. Forum 8 (2013), nr 1, str. 31–37,
http://m-hikari.com/imf/imf-2013/1-4-2013/tyszkaIMF1-4-2013-1.pdf.

[17] A. Tyszka, M. Sporysz, A. Peszek, *A conjecture on integer arithmetic which implies that there is an algorithm which to each Diophantine equation assigns an integer which is greater than the heights of integer (non-negative integer, rational) solutions, if these solutions form a finite set,* Int. Math. Forum 8 (2013), nr 1, str. 39–46,
http://m-hikari.com/imf/imf-2013/1-4-2013/tyszkaIMF1-4-2013-2.pdf.

[18] M. Waldschmidt, *Open Diophantine problems*, Mosc. Math. J. 4 (2004), nr 1, str. 245–305,
http://arxiv.org/abs/math/0312440.