Sieczne zespolone

Jarosław WRÓBLEWSKI, Wrocław

Jest to zapis odczytu wygłoszonego na XXXVII Szkole Matematyki Poglądowej *Algebraiczne Mocarstwo*, sierpień 2006.

Równanko pierwsze

Sieczną kojarzymy sobie zwykle z **widoczną na rysunku** prostą poprowadzoną przez dwa punkty krzywej. Jednakowoż ta sama sieczna może sobie istnieć w czysto **algebraicznej postaci**, a mianowicie w postaci równania prostej przechodzącej przez dwa punkty krzywej, również danej w postaci równania. Mówiąc o siecznej, wyjaśniamy wówczas, skąd się owe równania biorą. Jeśli nie ma rysunku na papierze, możemy widzieć krzywą i sieczną oczyma wyobraźni, ale do formalnego wyrachowania czegokolwiek na podstawie tych równań żaden rysunek nam nie jest potrzebny.

Oto przykład. Rozważmy równanie Pitagorasa

(1) $$a^2+b^2=c^2 \qquad a,b,c\in\mathbb{Z}.$$

Chcielibyśmy je zrozumieć jak najlepiej, czyli umieć uzyskać wszystkie jego rozwiązania, najlepiej w postaci parametrycznej.

Dzieląc obie strony równania (1) przez c^2 i przyjmując $x=a/c$, $y=b/c$ dochodzimy do równania

(2) $$x^2+y^2=1 \qquad x,y\in\mathbb{Q}.$$

Zauważamy, że jednym z rozwiązań równania jest

$$x_0=1,\quad y_0=0.$$

Można byłoby dalej rachować bez cienia geometrii w tle rachunków, ale tło geometryczne, nawet bez rysunku na papierze, pozwala zrozumieć dlaczego robimy to, co robimy.

Otóż naprawdę rozwiązujemy następujące zagadnienie: Na okręgu o równaniu (2) znaleźć punkty o obu współrzędnych wymiernych.

W dodatku jeden taki punkt, a mianowicie $(1,0)$ już nam się udało znaleźć.

Poprowadźmy przez punkt $(1,0)$ prostą nie będącą styczną do okręgu. Prosta ta przecina okrąg w jeszcze jednym punkcie. Jeżeli współczynnik kierunkowy tej prostej jest wymierny, to jej drugi punkt przecięcia z okręgiem ma obie współrzędne wymierne. I na odwrót: sieczna przecinająca okrąg w dwóch punktach wymiernych ma wymierny współczynnik kierunkowy.

Równanie takiej prostej możemy zapisać w postaci

$$(x,y)=(x_0,y_0)+t(m,n)=(1,0)+t(m,n),$$

czyli

$$x=x_0+mt=1+mt,\quad y=y_0+nt=nt.$$

Po wstawieniu powyższych wzorów do równiania (2) otrzymujemy

$$(1+mt)^2+(nt)^2=1.$$

Jest to równanie kwadratowe ze względu na t, które oczywiście ma rozwiązanie $t=0$, a drugim rozwiązaniem jest

$$t=\frac{-2\,m}{m^2+n^2}$$

prowadzące do

$$x=\frac{n^2-m^2}{m^2+n^2} \qquad y=\frac{-2mn}{m^2+n^2}.$$

Stąd już tylko krok do uzyskania znanej wszystkim parametryzacji rozwiązań równania Pitagorasa.

Równanko drugie

Rozważmy teraz następujące równanie:

(3) $$1+3a^2+b^2+2a\left(a^2+b^2\right)i=z^2$$
$$a,b\in\mathbb{Q}\setminus\{0\} \quad z\in\mathbb{Q}[i].$$

Jak widać, z założenia z ma być liczbą zespoloną o wymiernej części rzeczywistej i wymiernej części urojonej.

Przy tym nie jesteśmy już tak ambitni, aby chcieć sparametryzować wszystkie rozwiązania. Zadowolimy się możliwością wygenerowania nieskończenie wielu rozwiązań.

Czy potrafimy w ogóle wskazać jakiekolwiek rozwiązania tego równania?

Ależ tak. Komputer wyprodukuje nam trochę rozwiązań ze wspólnym $a=9/8$:

$$b=\pm\frac{237}{88},\qquad z=\pm\left(\frac{733}{176}+\frac{405\,i}{176}\right)$$
$$b=\pm\frac{1595}{1896},\qquad z=\pm\left(\frac{9509}{3792}+\frac{1119\,i}{1264}\right)$$
$$b=\pm\frac{4785}{248},\qquad z=\pm\left(\frac{12637}{496}+\frac{8181\,i}{496}\right)$$
$$b=\pm\frac{31}{264},\qquad z=\pm\left(\frac{1205}{528}+\frac{111\,i}{176}\right)$$

Powyżej mamy 16 rozwiązań, gdyż znaki $\pm$ przy b i z mogą być wybrane niezależnie.

Skoro nie zależy nam na wszystkich rozwiązaniach, to może ograniczmy się do rozwiązań z $a=9/8$.

Równanie (3) przyjmuje wówczas postać

(4) $$\frac{307}{64}+\frac{729\,i}{256}+\left(1+\frac{9\,i}{4}\right)b^2=z^2.$$

Możemy zastosować do równania (4) taką samą procedurę, jaką zastosowaliśmy do równania (2).

Wybieramy jedno rozwiązanie, np.

$$b_0=\frac{237}{88},\qquad z_0=\frac{733}{176}+\frac{405\,i}{176},$$

a następnie prowadzimy przez punkt (b_0,z_0) prostą

(5) $$b=b_0+t,\qquad z=z_0+\gamma t \qquad \gamma\in\mathbb{Q}[i],$$

która jest sieczną krzywej określonej równaniem (4).

Jednak mimo geometrycznego opisu przedstawionego wyżej, procedura ma w tym wypadku charakter czysto algebraiczny. Zarówno *krzywa* jak i *sieczna* są tworami dwuwymiarowymi w przestrzeni czterowymiarowej. Opis geometryczny stanowi jedynie inspirację rachunków, za które odpowiedzialność przejmuje czysta algebra.

Jednak algebraicznie wszystko działa tak, jak przy równaiu (2). Po wstawieniu b i z określonych wzorem (5) do równania (4) otrzymujemy równanie kwadratowe względem t mające oczywiście pierwiastek $t = 0$ oraz drugi pierwiastek

$$t = \frac{2\gamma z_0 - 2B_0 b_0}{B_0 - \gamma^2}, \quad \text{gdzie} \quad B_0 = 1 + \frac{9\,i}{4}.$$

Ale to jeszcze nie koniec, bo t, a co za tym idzie b, uzyskane powyższym wzorem, nie muszą być rzeczywiste.

Musimy więc odpowiedzieć na pytanie: Dla jakich $\gamma \in \mathbb{Q}[i]$ liczby b i t są rzeczywiste?

Po żmudnych przekształceniach odpowiedź na to pytanie jawi się w postaci: Dla takich $\gamma = x + yi,\ \ x, y \in \mathbb{Q}$, że

$$(6) \qquad -4977\,x + 4266\,x^2 - 1620\,x^3 + 6577\,y - 3792\,x\,y + 2932\,x^2\,y - 4266\,y^2 - 1620\,x\,y^2 + 2932\,y^3 = 0.$$

Pamiętajmy jednak, że nie tylko "dobre" γ wyznacza rozwiązanie równania (4), ale na odwrót: każde rozwiązanie równania (4) prowadzi do γ spełniającego równanie (6).

I tak

$$b_1 = -\frac{1595}{1896} \qquad z_1 = \frac{9509}{3792} + \frac{1119\,i}{1264}$$

prowadzi do

$$\gamma_1 = \frac{34561}{73714} + \frac{29529\,i}{73714}$$

oraz

$$b_2 = \frac{31}{264} \qquad z_2 = -\frac{1205}{528} - \frac{111\,i}{176}$$

prowadzi do

$$\gamma_2 = \frac{851}{340} + \frac{387\,i}{340}.$$

Krzywa (tym razem tradycyjna, jednowymiarowa na dwuwymiarowej płaszczyźnie) określona równaniem (6) jest krzywą trzeciego stopnia. Liczby γ_1 oraz γ_2 odpowiadają dwóm punktom na tej krzywej. Sieczna poprowadzona przez te dwa punkty przecina krzywą w trzecim punkcie odpowiadającym

$$\gamma_3 = \frac{160598426499}{89563302946} + \frac{78889762971\,i}{89563302946},$$

co prowadzi do

$$t = \frac{2\gamma_3 z_0 - 2B_0 b_0}{B_0 - \gamma_3^2} = -\frac{17859952585416279}{4677874919222516}$$

i w konsekwencji

$$b = b_0 + t = -\frac{956651800952265}{850522712585912}$$

oraz

$$z = z_0 + t\gamma_3 = -\frac{4561049905685197}{1701045425171824} - \frac{1806217413645861\,i}{1701045425171824}.$$

Otrzymaliśmy więc nowe rozwiązanie

$$a = 9/8$$
$$b = -\frac{956651800952265}{850522712585912}$$
$$z = -\frac{4561049905685197}{1701045425171824} - \frac{1806217413645861\,i}{1701045425171824}$$

równania (3).

Można udowodnić, że równanie (3) ma nieskończenie wiele rozwiązań.

Równanko trzecie

Teraz zajmiemy się najważniejszym zagadnieniem tego artykułu, a mianowicie równaniem

$$(7) \qquad A^4 - B^4 = C^4 - D^4 = E^4 - F^4,$$

gdzie A, B, C, D, E, F są liczbami całkowitymi dodatnimi.

Pierwszy przykład nietrywialnego rozwiązania:

$$421296^4 - 273588^4 = 415137^4 - 248289^4 = 401168^4 - 17228^4$$

podał Aurel J. Zajta w 1980 roku (praca opublikowana w Math. of Comp. 1983).

Ponieważ wszelakie sensowne rozważania heurystyczne sugerowały, że równanie (7) rozwiązań mieć nie powinno, a jeśli już, to skończenie wiele, przykład Zajty wydawał się być niczym więcej, jak tylko wybrykiem natury.

Jednak rozwój technik obliczeniowych umożliwił znalezienie kolejnych rozwiązań. Wiadomo, że istnieją dokładnie 4 rozwiązania w liczbach $A, B, C, D, E, F < 10^7$. Spośród 40 rozwiązań, które udało mi się znaleźć przez bezpośrednie (ale selektywne) przeszukanie, w największym występują liczby 14-cyfrowe. W tabeli na końcu artykułu zamieszczone są 23 rozwiązania w liczbach mniejszych od 10^{10}.

Naturalne jest więc pytanie: Czy równanie (7) ma nieskończenie wiele istotnie różnych nietrywialnych rozwiązań?

Na to pytanie twierdzącą odpowiedź uzyskaliśmy (Ajai Choudhry & JW) w roku 2006.

Równanie (7) jest równoważne równaniu

$$(8) \quad x_1 y_1 \left(x_1^2 + y_1^2\right) = x_2 y_2 \left(x_2^2 + y_2^2\right) = x_3 y_3 \left(x_3^2 + y_3^2\right)$$

po wykonaniu podstawień

$$x_1 = \frac{A+B}{2} \qquad y_1 = \frac{A-B}{2}$$
$$x_2 = \frac{C+D}{2} \qquad y_2 = \frac{C-D}{2}$$
$$x_3 = \frac{E+F}{2} \qquad y_3 = \frac{E-F}{2}$$

Z kolei każde rozwiązanie równania (3), w którym przyjmujemy $z = c + di$ prowadzi przez podstawienia

$$x_1 = |c + ad|, \qquad x_2 = |bc|, \qquad x_3 = |a + cd|,$$
$$y_1 = |bd|, \qquad y_2 = |ac - d|, \qquad y_3 = |b|$$

do rozwiązania równania (8).

Na przykład rozwiązanie równania (3) uzyskane z γ_3 daje

$$x_1 = \frac{52744355968294325}{13608363401374592}$$
$$y_1 = \frac{172792114167565511360527582516 5}{144677776924899574161996174348 8}$$
$$x_2 = \frac{4363336606506902131841914121205}{1446777769248995741619961743488}$$
$$y_2 = \frac{26599709841999885}{13608363401374592}$$
$$x_3 = \frac{11493497744966655189516021942465}{2893555538497991483239923486976}$$
$$y_3 = \frac{956651800952265}{850522712585912},$$

co po usunięciu wspólnego mianownika prowadzi do

$$x_1 = 773452977788803903574218354 30$$
$$y_1 = 238333950575952429462796665 54$$
$$x_2 = 601839531931986500943712292 58$$
$$y_2 = 390063058083033153221275114 14$$
$$x_3 = 792655016894252082035587720 17$$
$$y_3 = 224456299240308518715096135 36$$

oraz

$$A = 101178692836475633303701501984$$
$$B = 535119027212851474111421688 76$$
$$C = 991902590015019654164987406 72$$
$$D = 211776473848953347722437178 44$$
$$E = 101711131613456060075068385553$$
$$F = 568198717653943563320491584 81.$$

Otrzymaliśmy więc rozwiązanie równania (7) zawierające liczby 30-cyfrowe.

Najmniejsze rozwiązanie, które udało się wygenerować opisanymi metodami, zawiera liczby 24-cyfrowe.

Przedstawione powyżej rozważania były podstawą pierwszej wersji dowodu istnienia nieskończenie wielu rozwiązań równania (7). W wersji ostatecznej liczby zespolone już nie występują, jednak przez długi czas użycie algebraicznej manipulacji, którą określić można jako *sieczne zespolone*, było jedyną drogą generowania nowych rozwiązań i dowodu, że jest ich nieskończenie wiele.

A	B	C	D	E	F
335084	296668	265076	93436	264047	1169
421296	273588	415137	248289	401168	17228
854688	813396	747633	682161	614656	465236
3138156	2840232	2377876	500296	2376783	249999
27220940	24543080	20830065	6730545	20773068	39432
43134160	39597700	37607745	31601025	32721072	19453572
49734032	47450804	32004351	5106879	31999248	1829556
49888344	39566652	44400113	19439153	43986552	1772484
57218008	56255396	28999496	7923364	28962047	4144961
80325288	41563476	79714568	36280748	79087329	26275617
91785840	89603460	50547505	11071345	50518608	3231108
140326844	139033552	61413863	18878503	61306948	12960784
197237095	150215015	191610280	136159640	178105688	37694312
657153271	613063351	469658376	241846092	461665368	117778356
751888607	509011231	728659604	414173824	708852076	31047392
1180872001	1161828737	616132528	383720564	601308944	301870196
1596600137	1582784777	716243652	450436344	702011844	380055768
3071712177	2980091889	1860358392	1161850644	1805476184	828030484
4275254036	4274662012	660603913	271493129	660079796	263615324
4779990264	4779753552	628280072	478478672	625923087	473081841
6427460484	5799560808	5594408068	4483641784	4989936609	2584078431
6621888824	6399150812	4017771432	1956085212	3968658927	1208210001
9865447832	8250756572	8782377144	5772976932	8348157633	2076294399