

Niewidzialne dziury równań diofantycznych

Masza Vlasenko

(Instytut Matematyczny PAN)

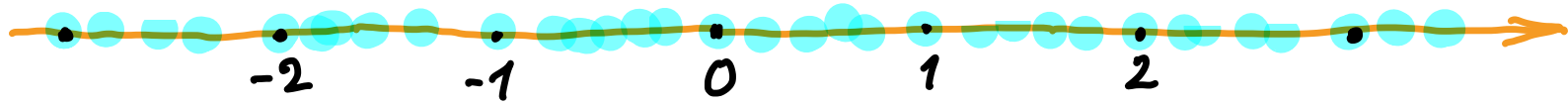
9. Kongres Młodych Matematyków
13 września 2024, Wrocław

Liczby wymierne

Liczby wymierne (ułameki)

np. $\frac{3}{4}$, $-\frac{1}{2}$, 0 , $\frac{17}{26}$, 3 , ...

są gęste wśród liczb rzeczywistych



t. zn. w jakkolwiek małym odcinku
osi liczbowej koniecznie znajdzie
się ułamek

Na płaszczyźnie :
punkt o współrzędnych wymiernych
nazywamy po prostu **wymiernym**
punktem

Ile punktów wymiernych może
być na linii prostej ?

Na płaszczyźnie:
punkt o współrzędnych wymiernych
nazywamy po prostu **wymiernym**
punktem

Ile punktów wymiernych może
być na linii prostej?

0, 1 lub ∞ (nieskończenie
wiele)

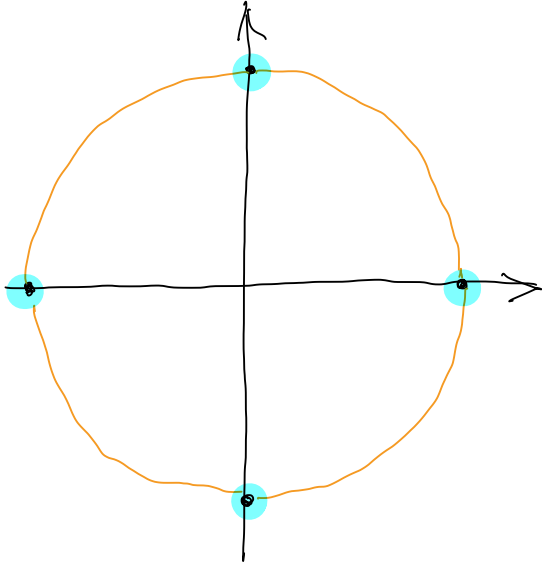
Np. $y = 2x + \sqrt{2}$

$$y = \sqrt{2}x$$

$$y = a x + b$$

z wymiernymi a, b

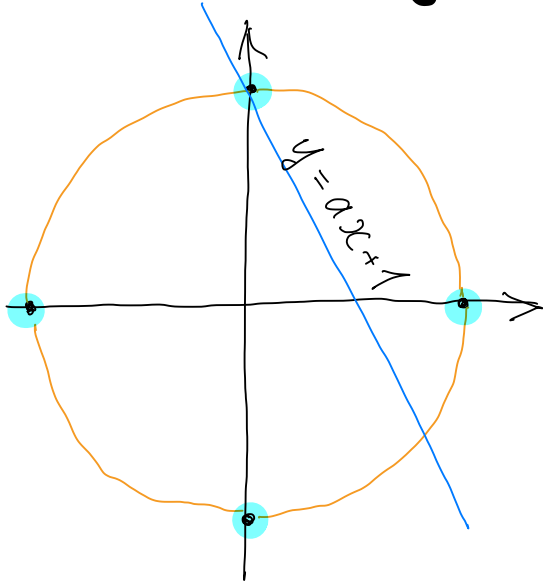
Punkty wymierne na okręgu



$$(\pm 1, 0) \quad (0, \pm 1)$$

$$x^2 + y^2 = 1$$

Punkty wymierne na okręgu

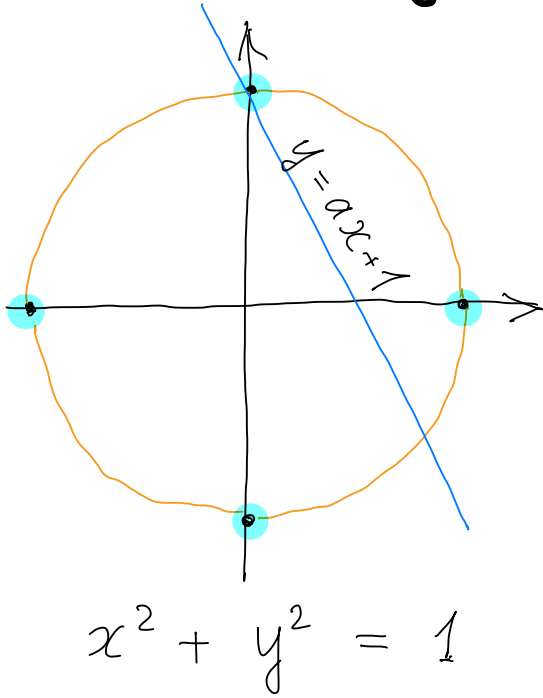


$$x^2 + y^2 = 1$$

$$(\pm 1, 0) \quad (0, \pm 1)$$

$$\begin{cases} y = a x + 1 \\ x^2 + y^2 = 1 \end{cases}$$

Punkty wymierne na okręgu



$$(\pm 1, 0) \quad (0, \pm 1)$$

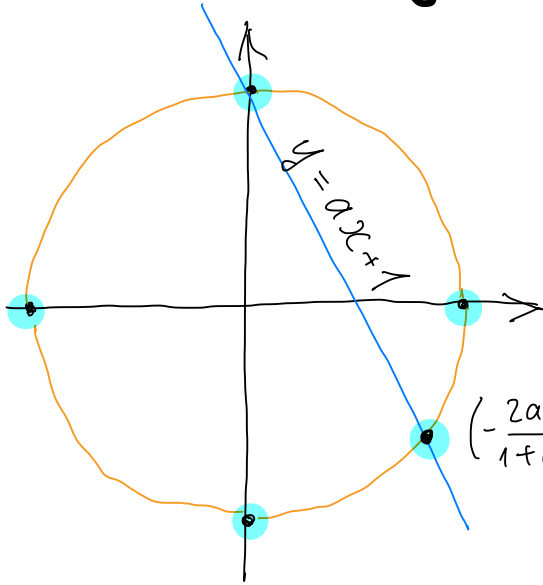
$$\begin{cases} y = ax + 1 \\ x^2 + y^2 = 1 \end{cases}$$

$$x^2 + (ax + 1)^2 = 1$$

$$(1 + a^2)x^2 + 2ax = 0$$

$$x = -\frac{2a}{1 + a^2}$$

Punkty wymierne na okręgu



$$x^2 + y^2 = 1$$

$$(\pm 1, 0) \quad (0, \pm 1)$$

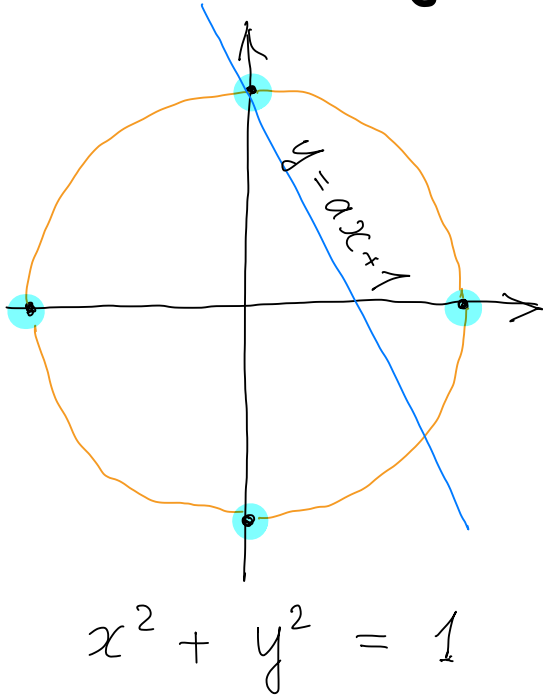
$$\begin{cases} y = ax + 1 \\ x^2 + y^2 = 1 \end{cases}$$

$$x^2 + (ax + 1)^2 = 1$$

$$(1 + a^2)x^2 + 2ax = 0$$

$$x = -\frac{2a}{1+a^2} \rightsquigarrow y = \pm \frac{1-a^2}{1+a^2}$$

Punkty wymierne na okręgu



$$(\pm 1, 0) \quad (0, \pm 1)$$

$$\begin{cases} y = ax + 1 \\ x^2 + y^2 = 1 \end{cases}$$

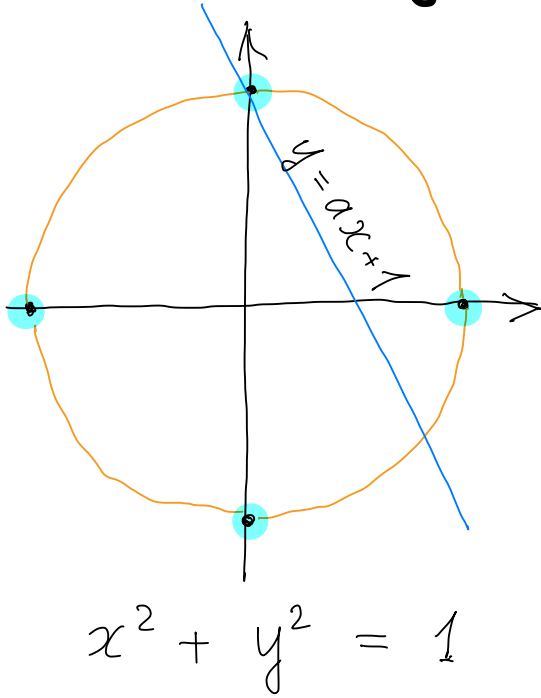
$$x^2 + (ax + 1)^2 = 1$$

$$(1 + a^2)x^2 + 2ax = 0$$

$$x = -\frac{2a}{1 + a^2} \leadsto y = \pm \frac{1 - a^2}{1 + a^2}$$

Kiedy pochylenie a jest wymierne, to jest wymierny punkt na okręgu.

Punkty wymierne na okręgu



$$(\pm 1, 0) \quad (0, \pm 1)$$

$$\begin{cases} y = ax + 1 \\ x^2 + y^2 = 1 \end{cases}$$

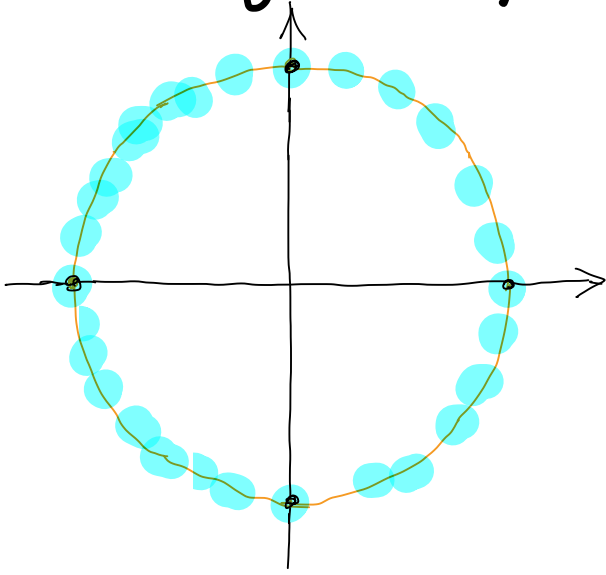
$$x^2 + (ax + 1)^2 = 1$$

$$(1 + a^2)x^2 + 2ax = 0$$

$$x = -\frac{2a}{1 + a^2} \quad \leadsto \quad y = \pm \frac{1 - a^2}{1 + a^2}$$

Kiedy pochylenie a jest wymierne, to jest wymierny punkt na okręgu. I odwrotnie!
Tak dostajemy **wszystkie punkty wymierne**.

Trójki pitagorejskie

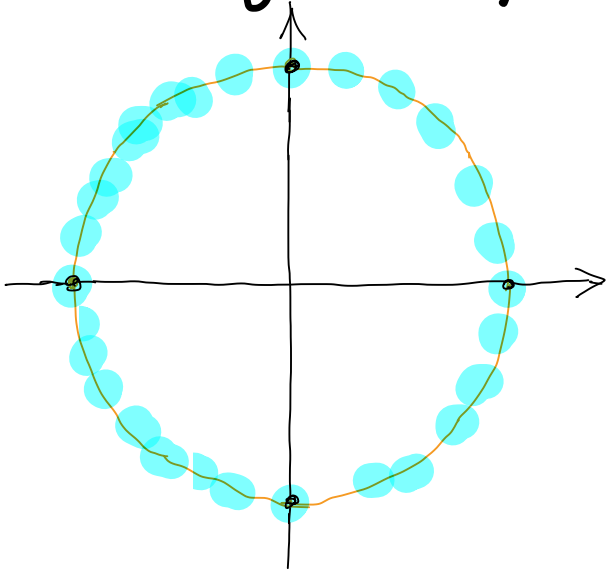


$$\left(\frac{2a}{1+a^2}, \frac{1-a^2}{1+a^2} \right)$$

wymierne

$$a = \frac{m}{n}$$

Trójki pitagorejskie



$$\left(\frac{2a}{1+a^2}, \frac{1-a^2}{1+a^2} \right)$$

wymierne

$$a = \frac{m}{n}$$

$$\left(\frac{2 \frac{m}{n}}{1 + \frac{m^2}{n^2}} \right)^2 + \left(\frac{1 - \frac{m^2}{n^2}}{1 + \frac{m^2}{n^2}} \right)^2 = 1$$

$$\left(\frac{2mn}{n^2 + m^2} \right)^2 + \left(\frac{n^2 - m^2}{n^2 + m^2} \right)^2 = 1$$

$$(2mn)^2 + (n^2 - m^2)^2 = (n^2 + m^2)^2$$

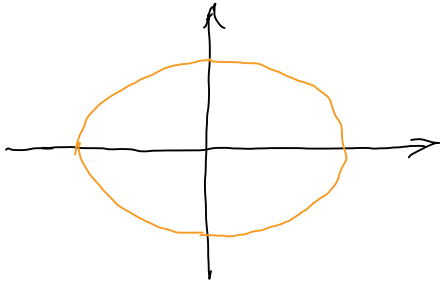
Krzywe drugiego stopnia

$$a_{20}x^2 + a_{11}xy + a_{02}y^2 + a_{10}x + a_{01}y + a_{00} = 0$$

$$a_{20}, a_{11} \text{ lub } a_{02} \neq 0$$

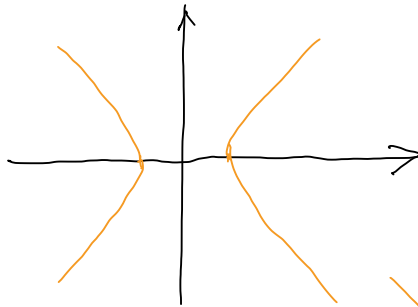
Np. elipsa,

$$\frac{x^2}{9} + \frac{y^2}{4} = 1$$



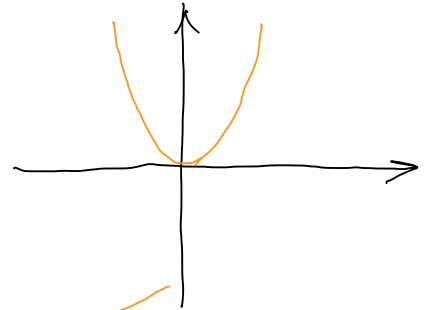
hiperbola,

$$x^2 - y^2 = 1$$



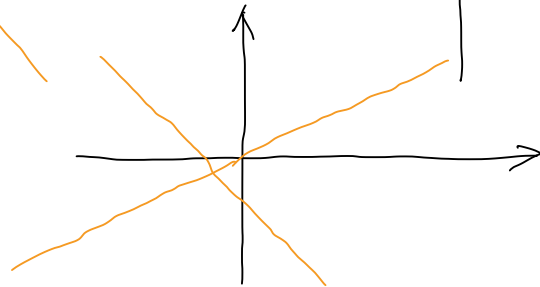
parabola

$$y = x^2$$

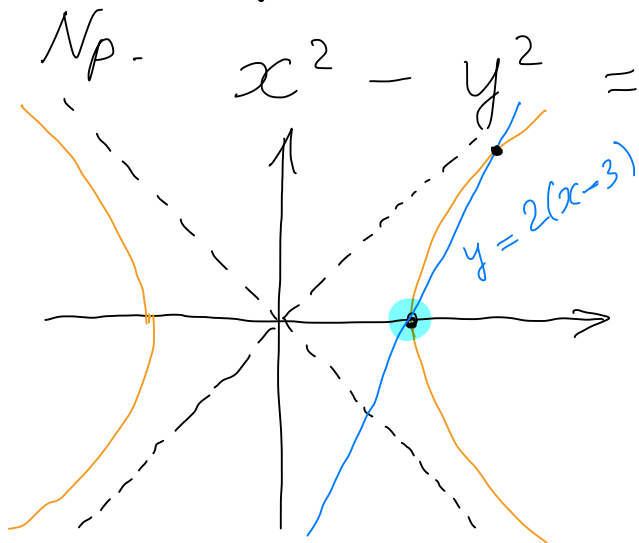


lub para prostych

$$(x - 2y)(x + y + 1) = 0$$



Na krzywych drugiego stopnia działa ta sama zasada co na okręgu: jeżeli mamy jeden punkt wymierny, to dostaniemy wszystkie inne rysując proste o wymiernym pochyleniu przez ten pierwszy punkt.



$$\begin{cases} y = a(x-3) \\ x^2 - y^2 = 9 \end{cases}$$

$$x^2 - a^2(x-3)^2 = 9$$

$$(1-a^2)x^2 + 6a^2x - 9(a^2+1) = 0$$

$$x = \frac{-6a^2 \pm 6}{2(1-a^2)} \quad x_1 = 3 \quad x_2 = 3 \frac{a^2+1}{a^2-1}$$

Podsumujemy:

- na linii prostej o wymiernych współczynnikach zawsze mamy nieskończenie wiele punktów wymiernych

$$a_{10}x + a_{01}y + a_{00} = 0$$

- na wymiernej krzywej drugiego stopnia może nie być punktów wymiernych, ale jeżeli są, to jest ich zawsze nieskończenie wiele

$$a_{20}x^2 + a_{11}xy + a_{02}y^2 + a_{10}x + a_{01}y + a_{00} = 0$$

Krzywe trzeciego stopnia

$$a_{30}x^3 + a_{21}x^2y + a_{12}xy^2 + a_{03}y^3 + a_{20}x^2 + a_{11}xy + a_{02}y^2 + a_{10}x + a_{01}y + a_{00} = 0$$

$$a_{30}, a_{21}, a_{12} \text{ lub } a_{03} \neq 0$$

Krzywe trzeciego stopnia

$$a_{30}x^3 + a_{21}x^2y + a_{12}xy^2 + a_{03}y^3 + a_{20}x^2 + a_{11}xy + a_{02}y^2 + a_{10}x + a_{01}y + a_{00} = 0$$

$$a_{30}, a_{21}, a_{12} \text{ lub } a_{03} \neq 0$$

Skupimy się na

krzywych eliptycznych

$$y^2 = \underbrace{x^3 + ax^2 + bx + c}$$

wielomian 3 stopnia
bez pierwiastków
wielokrotnych

Krzywe trzeciego stopnia

$$a_{30} x^3 + a_{21} x^2 y + a_{12} x y^2 + a_{03} y^3 + a_{20} x^2 + a_{11} x y + a_{02} y^2 + a_{10} x + a_{01} y + a_{00} = 0$$

$$a_{30}, a_{21}, a_{12} \text{ lub } a_{03} \neq 0$$

Skupimy się na

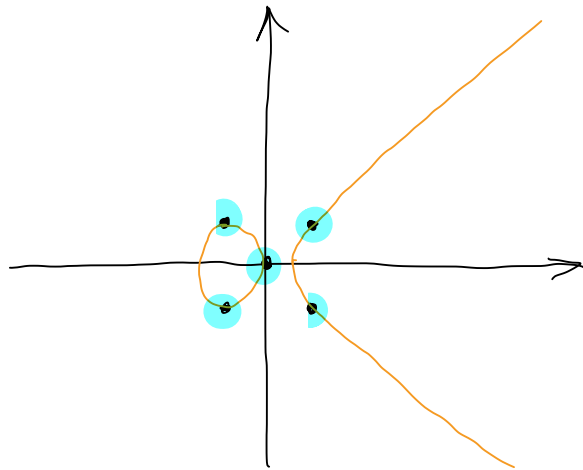
krzywych eliptycznych

$$y^2 = \underbrace{x^3 + a x^2 + b x + c}_{\text{wielomian 3 stopnia bez pierwiastków wielokrotnych}}$$

wielomian 3 stopnia
bez pierwiastków
wielokrotnych

Np.

$$y^2 = x^3 + x^2 - x$$



Twierdzenie

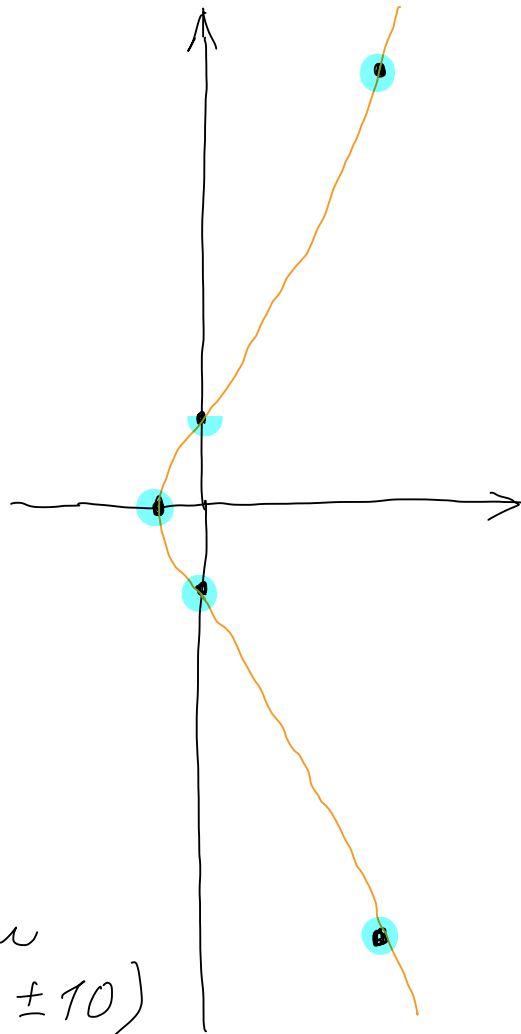
(Barry Mazur 1978)

Na wymiernej krzywej
eliptycznej może być
dokładnie

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 15

lub ∞ punktów
wymiernych

Np. $y^2 = x^3 + x^2 + 4x + 4$
ma dokładnie pięć punktów
wymiernych: $(-1, 0)$, $(0, \pm 2)$, $(4, \pm 10)$

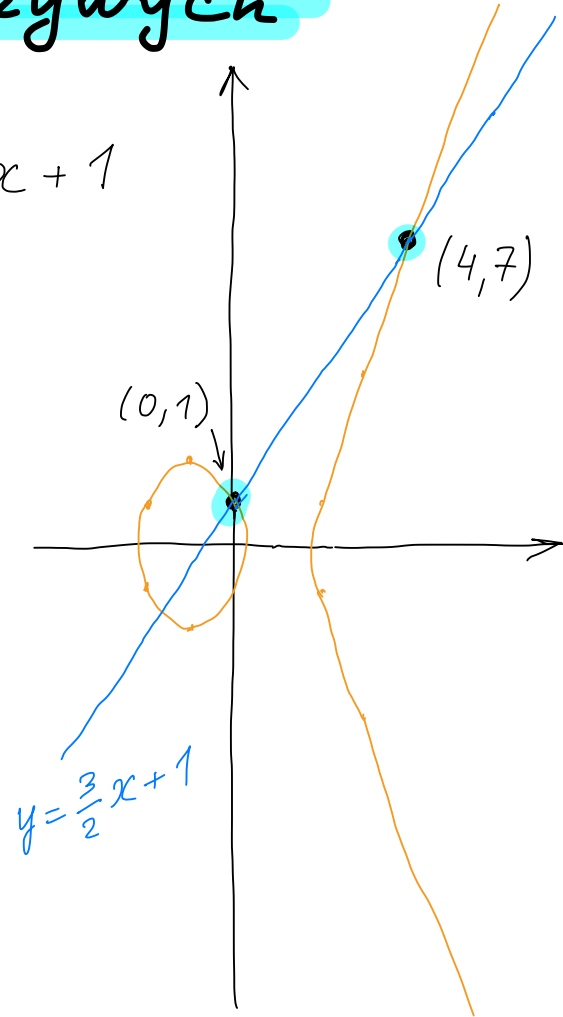


Punkty wymierne na krzywych eliptycznych

Linia prosta przez dwa punkty wymierne nie symetryczne według osi poziomej przecina krzywą w trzecim punkcie.

Z wzorów Viète'a wynika że ten nowy punkt jest wymierny.

$$y^2 = x^3 - 4x + 1$$



Punkty wymierne na krzywych eliptycznych

Np.

$$y = \frac{3}{2}x + 1$$

$$\left(\frac{3}{2}x + 1\right)^2 = x^3 - 4x + 1$$

$$x^3 - \frac{9}{4}x^2 - 7x = 0$$

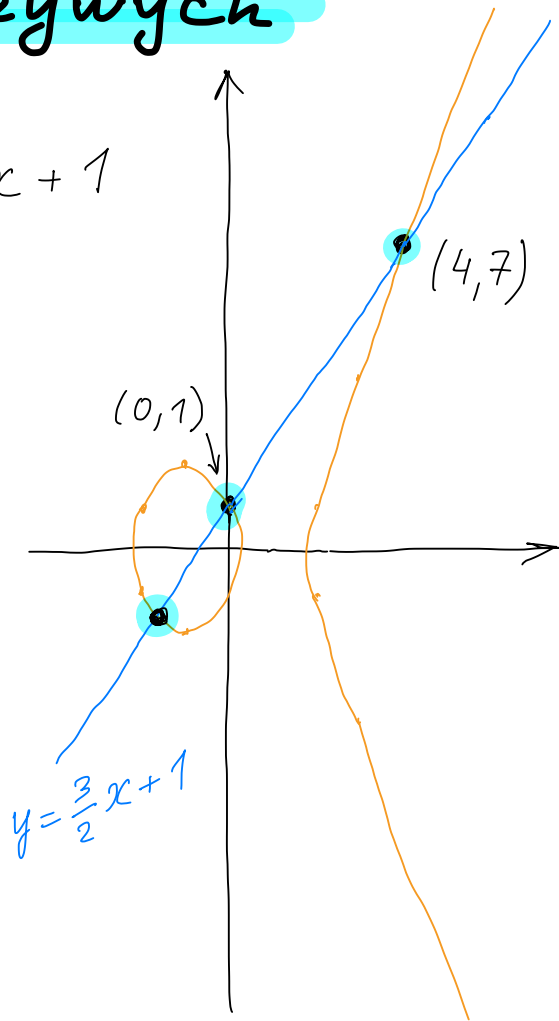
$$x(x - 4)\left(x + \frac{7}{4}\right) = 0$$

$$\swarrow$$
$$(0, 1)$$

$$\swarrow$$
$$(4, 7)$$

$$\swarrow$$
$$\left(-\frac{7}{4}, -\frac{13}{8}\right)$$

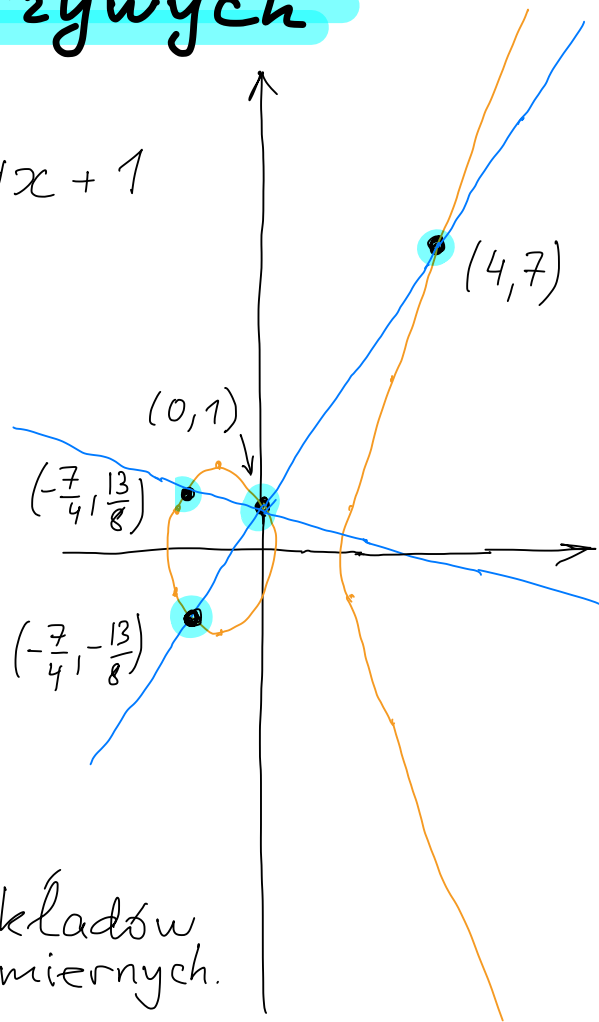
$$y^2 = x^3 - 4x + 1$$



Punkty wymierne na krzywych eliptycznych

Dla każdego punktu (x, y) na krzywej mamy też punkt $(x, -y)$ co pozwala budować nowe linie proste i nowe punkty wymierne.

$$y^2 = x^3 - 4x + 1$$



Na odmianę od poprzednich przykładów ta krzywa ma ∞ punktów wymiernych.

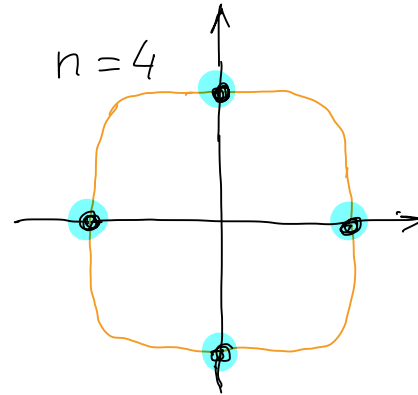
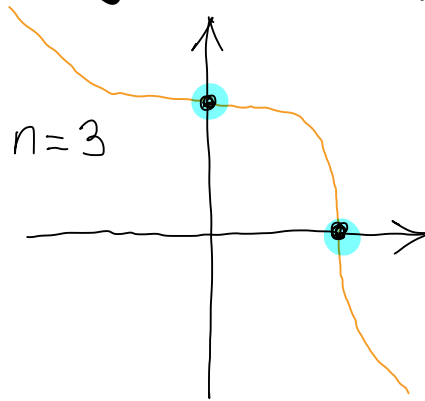
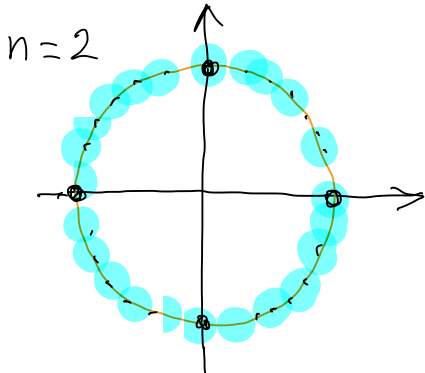
Wielkie Twierdzenie Fermata

(Andrew Wiles 1995)

Dla $n \geq 3$ na krzywej

$$x^n + y^n = 1$$

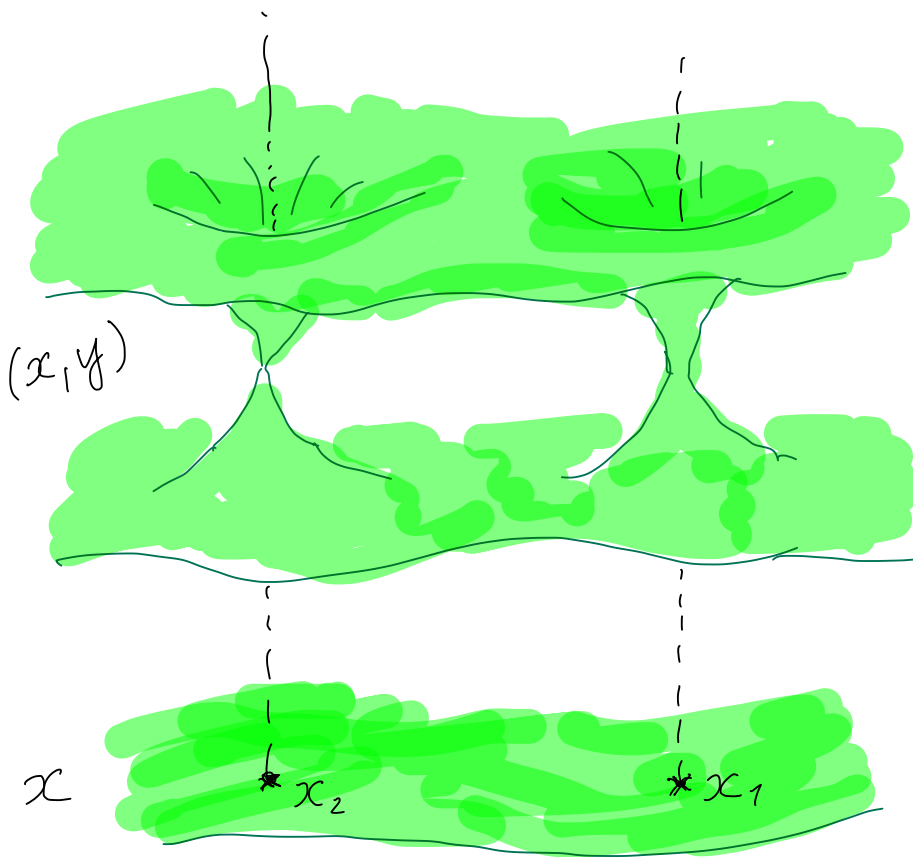
nie ma punktów wymiernych
o niezerowych współrzędnych.



Czy te
krzywe
są
różne
od
okręgu?
($n=2$)

"Niewidzialne dziury"

"Niewidzialne dziury"



Patrzemy na
zbiór par liczb
zespółonych (x, y)
takich że

$$y^2 = x^3 - 4x + 1$$

ten wielomian
ma pierwiastki

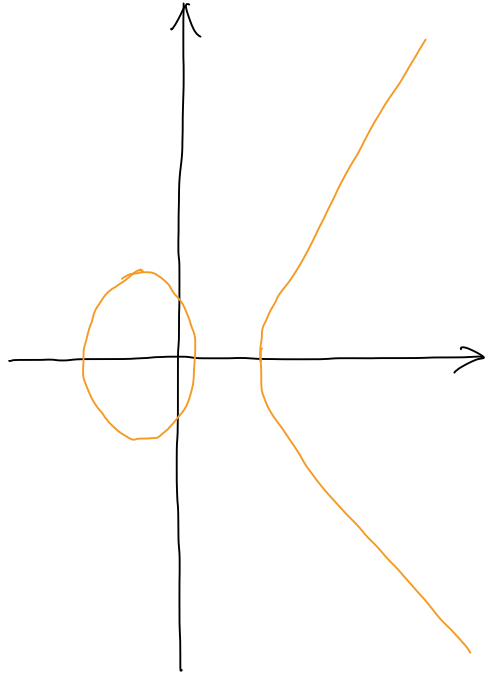
$$x_1 = -2.11490...$$

$$x_2 = 0.25410...$$

$$x_3 = 1.86080...$$

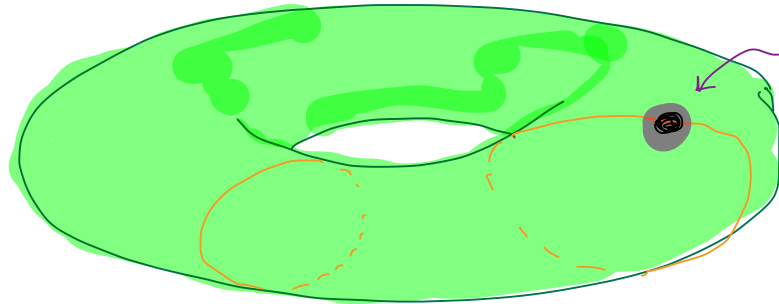
"Niewidzialne dziury"

$$y^2 = x^3 - 4x + 1$$



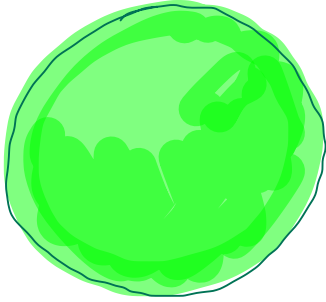
To jest słabo wyobrażalne
ale ...

zbiór punktów zespolonych
tej krzywej można
"dokleić" **jednym punktem**
tak że dostaniemy
paczek z jedną dziurką

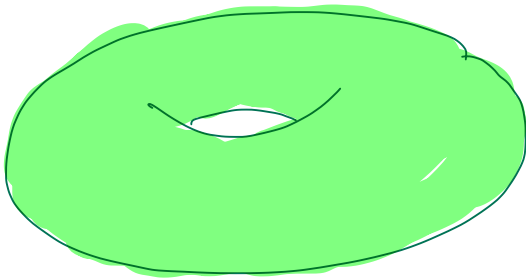


"Niewidzialne dziury"

$$x^2 + y^2 = 1$$



$$x^3 + y^3 = 1$$



$$x^4 + y^4 = 1$$



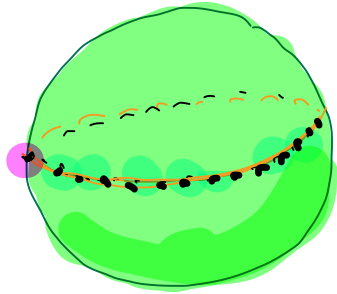
Ilość dziurek w
pęczku zespolonych
punktów krzywej
nazywa się jej
genusem

Twierdzenie (Gerd Faltings 1983)

Krzywa genu większego od 1
ma skończoną ilość punktów
wymiernych.

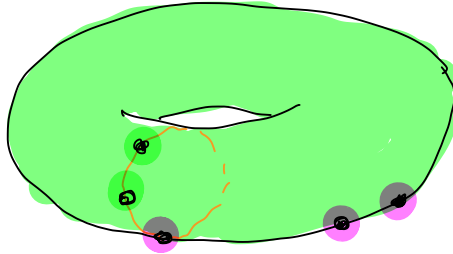
Ale jak je policzyć?

$$x^2 + y^2 = 1$$



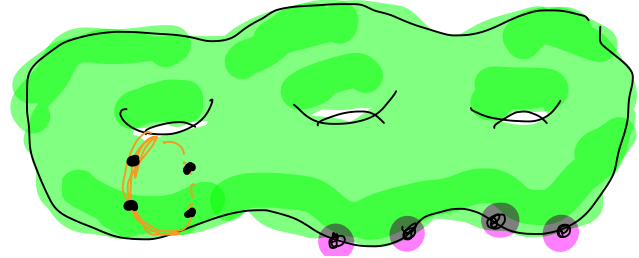
genus 0
 ∞ punktów

$$x^3 + y^3 = 1$$



genus 1
3 punkty

$$x^4 + y^4 = 1$$



genus 3
4 punkty

Rozwiązania w resztach z dzielenia przez liczbę pierwszą

$$p = 2, 3, 5, 7, \dots$$

Np. $x^4 + y^4 = 1$

$p = 3$

$x \backslash y$	0	1	2
0			
1			
2			

 pary reszt x, y
 takich że
 $x^4 + y^4 - 1$ jest
 podzielne
 przez 3

np. $0^4 + 2^4 - 1 = 15 = 3 \cdot 5$

$p = 5$

$x \backslash y$	0	1	2	3	4
0					
1					
2					
3					
4					

$p = 7$

$x \backslash y$	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

$$3^4 + 4^4 - 1 = 336 = 7 \cdot 48$$

Twierdzenie (Claude Chabauty 1941
Robert Coleman 1985)

Dla krzywej genusu $g \geq 2$
i każdej liczby pierwszej $p > 2g$
mamy

$$\text{ilość punktów wymiernych na krzywej} \leq (2g - 2) + \text{ilość rozwiązań w resztach od dzielenia przez } p$$

Twierdzenie (Claude Chabauty 1941
Robert Coleman 1985)

Dla wymiernej krzywej genusu $g \geq 2$ *

i każdej liczby pierwszej $p > 2g$
mamy

$$\text{ilość punktów wymiernych na krzywej} \leq (2g - 2) + \text{ilość rozwiązań w resztach od dzielenia przez } p$$

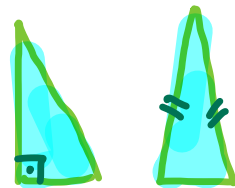
* Uwaga: krzywa w tym Twierdzeniu ma spełniać warunek techniczny (ranga jej Jakobianu ma być $< g$) oraz liczba p ma być taka, że krzywa ma "dobrą redukcję", co wyklucza skończony zbiór liczb pierwszych. Matematycy umieją sprawdzać to.

To trudne Twierdzenie  $\leq$  + 
pomogło japończykom Hirokawie i
Matsumurze rozwiązać następujący
problem:

Ile istnieje par trójkątów
o bokach wymiernych takich
że

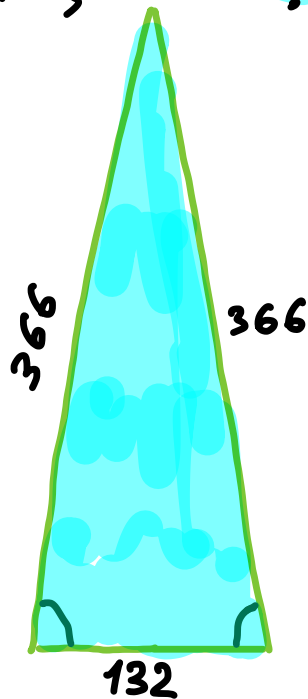
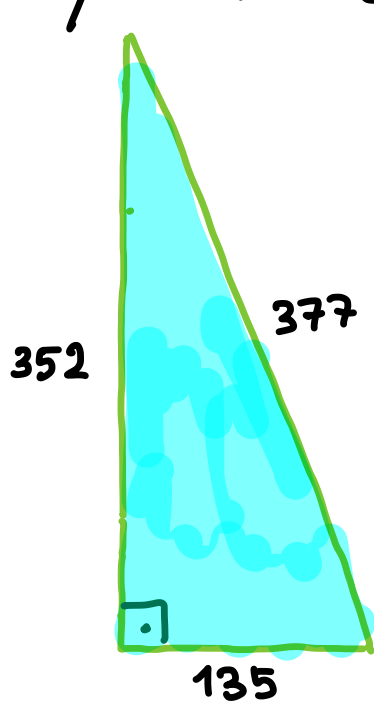
- jeden trójkąt jest prostokątny a drugi równoramienny
- mają równe obwody
- mają równe pola

?



Odpowiedź (Yoshinosuke Hirakawa
Hideki Matsumura 2018)

Z dokładnością
do podobieństwa istnieje jedyna taka
para trójkątów!



$$\text{Pole} = \frac{135 \cdot 352}{2}$$

$$= \frac{132 \cdot 360}{2}$$

$$= 23760$$

$$\text{Obwód} = 135 + 352 + 377$$

$$= 132 + 2 \cdot 366$$

$$= 864$$

Obliczenia Hirakawy i Matsumury
można przeczytać w ich artykule
"A unique pair of triangles"
Journal of Number Theory 194 (2019)
297 - 302

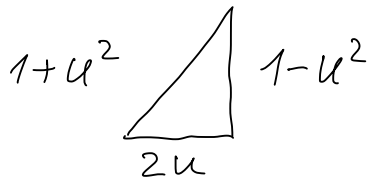
albo na

<https://arxiv.org/abs/1809.09936>

Dziękuję za uwagę!

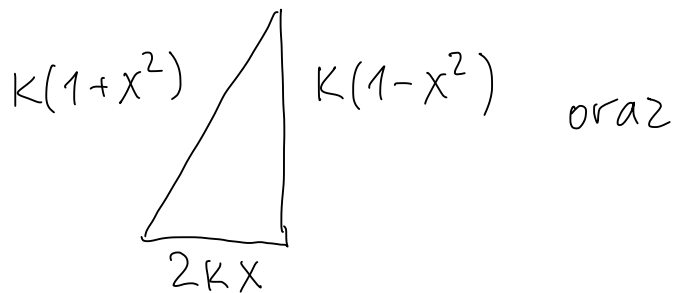
Bonus: szkic dowodu Hirakawy-Matsumury

- każdy trójkąt prostokątny o wymiernych bokach jest podobny do trójkąta

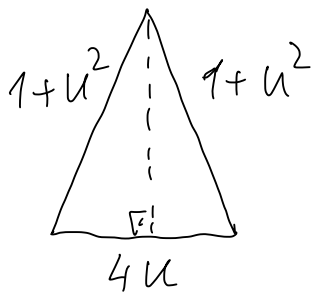


dla niektórego wymiernego
 $0 < u < 1$

- poszukiwana parę można opisać jak

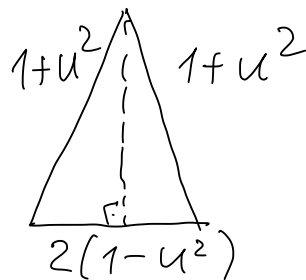


oraz



wariant I

lub



wariant II

dla niektórych wymiernych
 $K > 0$, $0 < u, x < 1$

Pokażemy obliczenia dla wariantu II

$$\begin{cases} (1+x) 2k = 4 & \Leftrightarrow \text{równe obwody} \\ k^2 x (1-x^2) = 2u(1-u^2) & \Leftrightarrow \text{równe pola} \end{cases}$$

$x = \frac{2}{k} - 1$ podstawiamy w drugie równanie

$$k^2 \left(\frac{2}{k} - 1 \right) \left(1 - \left(\frac{2}{k} - 1 \right)^2 \right) = 2u(1-u^2)$$

$$(2-k)(k^2 - 4 + 4k - k^2) = 2ku(1-u^2)$$

$$2(2-k)(k-1) = ku(1-u^2)$$

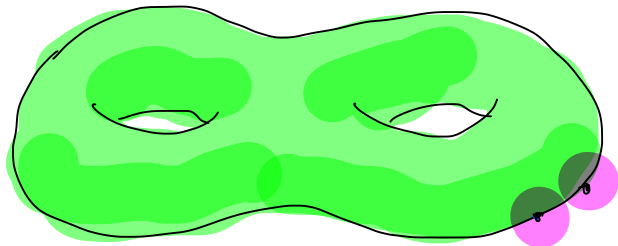
$$2k^2 - (u^3 - u + 6)k + u = 0$$

popatrzmy na to jak na równanie stopnia 2 dla k . Jeżeli ma ono wymierne rozwiązania to dyskryminant jest kwadratem

to już
krzywa
na
płaszczyźnie
nie
współrzedny-
mi (k, u)

$\Rightarrow$ Istnieje wymierna liczba s taka że

$$s^2 = (u^3 - u + 6)^3 - 32 \leftarrow$$



Ta krzywa ma genus 2 i spełnia warunki Twierdzenia Chabauty - Coleman.

Mamy 6 rozwiązań w resztach od dzielenia przez 5, dlatego

$p=5$

$u \backslash s$	0	1	2	3	4
0			■	■	■
1			■	■	
2					
3					
4			■	■	■

ilość punktów wymiernych $\leq 2 \cdot 2 - 2 + 6 = 8$

artykułu Z pomocą komputera autorzy znaleźli 8 punktów wymiernych

$$(u, s) = (0, \pm 2) \quad (1, \pm 2) \quad (-1, \pm 2) \quad \left(\frac{5}{6}, \pm \frac{217}{216} \right)$$

*nie zwracamy tu uwagi na "punkty na nieskończoności" ● ●

Pierwsze 3 pary nie mają $0 < u < 1$
i dlatego nie odpowiadają trójkątom.

Z ostatniej pary dostaniemy punkty

$$(k, x, u) = \left(\frac{27}{16}, \frac{5}{27}, \frac{5}{6} \right) \text{ i } \left(\frac{32}{27}, \frac{11}{16}, \frac{5}{6} \right)$$

które dają tą samą parę trójkątów
(proszę sprawdzić!)

Postępowanie dla wariantu I
jest podobne i nie daje żadnych
nowych par trójkątów.