

Po co więc te całe krzywe eliptyczne? Po prostu najszybsze algorytmy rozwiązujące logarytm dyskretny dla losowej krzywej postaci $K_{\mathbb{F}_p}$ są jeszcze wolniejsze niż algorytmy dla grupy \mathbb{F}_p podobnego rozmiaru. Konkretnie dla krzywych eliptycznych wszystkie znane ogólne algorytmy rozwiązujące problem logarytmu dyskretnego działają w czasie

$$2^{O(\ln p)} \gg 2^{O(\sqrt[3]{\ln p \ln \ln^2 p})}.$$

Z takimi deklaracjami należy uważać. Uczciwiej byłoby napisać *na dzień dzisiejszy bezpieczniejszy*, gdyż nie znamy żadnych ścisłych dolnych oszacowań na czas rozwiązywania tych problemów. W każdej chwili może ktoś znaleźć jakiś efektywniejszy algorytm i sytuacja może się odwrócić.

Oznacza to, że każdy protokół kryptograficzny, oparty o problem logarytmu dyskretnego, staje się *bezpieczniejszy* bez zwiększenia p (a więc bez zwiększenia rozmiaru kluczy), jeśli tylko zmienimy grupę, z którą pracujemy, z \mathbb{F}_p z mnożeniem na $K_{\mathbb{F}_p}$ z dodawaniem punktów. Dokładnie z tego powodu już nie jest popularne używanie podpisu cyfrowego DSA (z roku 1991), a powszechnie używa się podpisu ECDSA (z roku 1999) – czyli jego odpowiednika, ale opartego o krzywe eliptyczne.

A jednak ta geometria algebraiczna gdzieś się przydaje!

Wyniki XXXV Ogólnopolskiego Sejmiku Matematyków, Szczyrk, 14–17 VI 2018

Konkurs polega na przedstawieniu opracowania jednego z tematów zaproponowanych (wraz z bibliografią) przez Jury lub tematu własnego oraz – w przypadku zakwalifikowania się do finału – krótkim, publicznym zreferowaniu tego opracowania.

Sejmiki organizuje Pracownia Matematyki i Informatyki Pałacu Młodzieży w Katowicach we współpracy z Uniwersytetem Śląskim; www.spinor.edu.pl

Jury w składzie: prof. dr hab. Maciej Sablik – przewodniczący, dr Paweł Błaszczyk, dr Anna Brzeska, dr Dawid Czapla, mgr Żywilla Fechner, dr hab. Mieczysław Kula, dr Agnieszka Kulawik, dr Marian Podhorodyński, dr Anna Szczerba-Zubek, dr Hanna Wojewódka **postanowiło przyznać następujące wyróżnienia:**

- I miejsce: Bartosz Bartoszek** – I LO w Zduńskiej Woli za pracę *Funkcje potęgowe (j, k) symetryczne*, opiekun: dr inż. Renata Długosz;
II miejsce: Filip Rękawek – Katolickie LO w Garwolinie za pracę *O trójkątach kappa i ich własnościach*, opiekun: mgr Zofia Burno;
III miejsce: Krzysztof Witkowski – I LO w Gliwicach za pracę *O własnościach sum Freya*, opiekun: mgr Joanna Olesińska;
IV miejsce Gabriela Pietras – Publiczna Szkoła Podst. w Leszczynie, za pracę *Wokół twierdzenia Morse’a–Hedlunda*, opiekun mgr Martha Łącka;
V miejsce Jakub Michalec– LO Zakonu Pijarów w Krakowie za pracę *Paradoksy nieskończoności*, opiekun: Jolanta Przybylska.

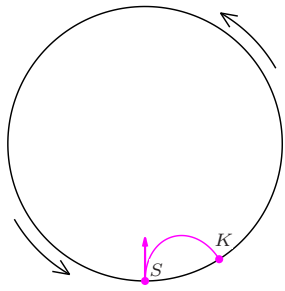
W głosowaniu publiczności na najlepszą prezentację **nauczyciele nagrodzili Rafała Loskę** – VIII LO w Katowicach, praca *Jak obliczyć pole figury płaskiej?*,
a uczniowie Pawła Tyrnę – LO Towarzystwa Szkolnego w Bielsku–Białej, praca *Matematyczne podstawy projektowania origami*.

Problemy sztucznej grawitacji

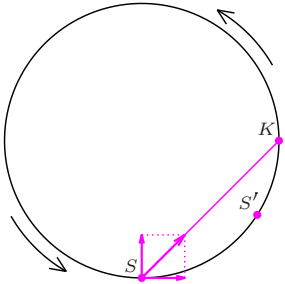
Szymon CHARZYŃSKI

Podróże w kosmos to marzenie większości dzieci i licznej grupy dorosłych (wliczając autora). Niestety, okazję do zrealizowania tych marzeń miała, jak na razie, bardzo nieliczna grupa ludzi, a najdalsze loty załogowe odbyte do tej pory to te z przełomu lat sześćdziesiątych i siedemdziesiątych dwudziestego wieku w ramach programu Apollo, dzięki któremu ludzie kilkakrotnie lądowali na Księżycu. Z kolei najdłuższe pobyty w przestrzeni kosmicznej były udziałem załóg stacji kosmicznych krążących na niskiej orbicie okołozemskiej (kilkaset km nad jej powierzchnią) i trwały kilka miesięcy. Pomimo tego, że podbój kosmosu przez gatunek ludzki jest ciągle jeszcze w powijakach, to wizjonerzy snują ambitne plany kolonizacji innych planet, zakładania na stałe zamieszkałych baz w przestrzeni i wysyłania załogowych statków nawet poza Układ Słoneczny.

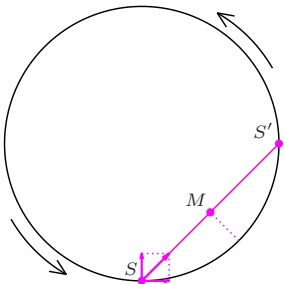
Te kilkadziesiąt lat doświadczeń z lotami kosmicznymi nauczyły nas, z jakimi problemami przyjdzie się mierzyć konstruktorom pojazdów przyszłości i ich załogom. Jednym z nich jest problem ciężenia, a raczej jego braku. Długie pozostawanie w stanie nieważkości ma dla organizmu ludzkiego różne, bardzo negatywne skutki zdrowotne. Dlatego wizjonerzy planujący długie podróże



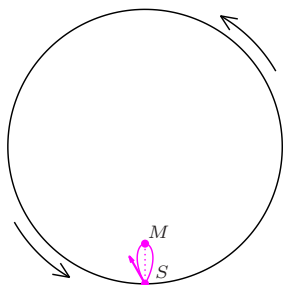
Rys. 1



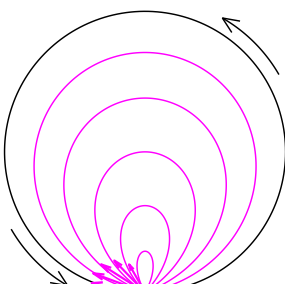
Rys. 2



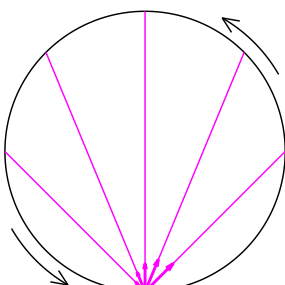
Rys. 3



Rys. 4



Rys. 5



Rys. 6

kosmiczne muszą zapewnić podróżnikom jakąś formę ciężenia. Nazywa się to czasami niezbyt trafnie *sztuczną grawitacją*. W tym artykule zajmiemy się analizą jednej z hipotetycznych metod zapewniania ciężenia pasażerom stacji i pojazdom kosmicznych. Jest to jeden z najprostszych i oczywistych pomysłów zastąpienia grawitacji siłą odśrodkową.

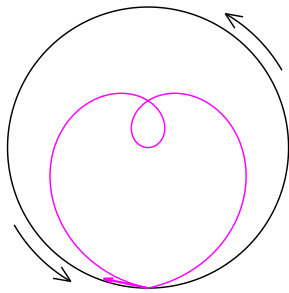
Wyobraźmy sobie pojazd w kształcie walca wirujący wokół swojej osi. Na dowolny obiekt spoczywający na wewnętrznej powierzchni takiego walca będzie działała siła bezwładności dociskająca go do tej powierzchni, dana wzorem $F = m \frac{v^2}{R}$, gdzie v to prędkość punktu na obwodzie walca, a R to promień.

Siła ta jest proporcjonalna do masy m , a współczynnik proporcjonalności $\frac{v^2}{R}$ zastępuje przyspieszenie grawitacyjne. Aby osoba stojąca na wewnętrznej powierzchni wirującego walca odczuwała przyspieszenie równe przyspieszeniu ziemskiemu g , to musi być spełniony warunek $\frac{v^2}{R} = g$. Oznacza to, że walec o zadanym promieniu R musi wirować z prędkością $v = \sqrt{gR}$, co przelicza się na okres obrotu $T = 2\pi \sqrt{\frac{R}{g}}$, tak aby iloczyn prędkości i okresu był równy obwodowi walca $v \cdot T = 2\pi R$. Widzimy więc, że zarówno prędkość, jak i okres rosną proporcjonalnie do \sqrt{R} . Dla $R = 50$ m mamy, na przykład, $v \approx 22 \frac{\text{m}}{\text{s}}$ i $T \approx 14$ s, a dla $R = 100$ m mamy $v \approx 31 \frac{\text{m}}{\text{s}}$ i $T \approx 20$ s.

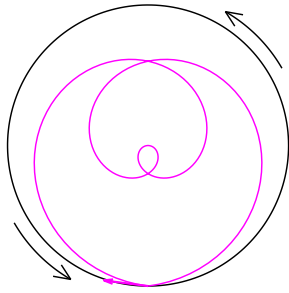
Mieszkaniec tak skonstruowanego statku będzie jednak mógł zauważyć pewne różnice między stałym polem grawitacyjnym na powierzchni Ziemi a sztucznym ciężeniem wywołanym siłą odśrodkową. Opiszemy teraz szczegółowo, co będzie się działo z podrzucanymi przedmiotami, co jest istotne dla mieszkańca, który chciałby umilić sobie czas żonglowaniem lub grą w ping-ponga, tenisa, piłkę nożną czy siatkówkę.

Zacznijmy od najprostszego eksperymentu: podrzucimy piłkę pionowo do góry. Na Ziemi spodziewalibyśmy się, że spadnie nam z powrotem do ręki, poruszając się w górę i w dół wzdłuż tej samej prostej pionowej linii. Niestety, ta intuicja zawodzi nas we wnętrzu wirującego walca. Tor lotu podrzuconej pionowo piłki (z prędkością początkową prostopadłą do powierzchni walca) będzie wyglądał jak na rysunku 1. Piłka wyrzucona w punkcie S spadnie w punkcie K , znajdującym się dalej w kierunku, w którym wiruje walec (tutaj przeciwnie do kierunku ruchu wskazówek zegara). Efekt ten można wyjaśnić działaniem siły Coriolisa, która pojawia się, kiedy obiekt w układzie obracającym się zmienia odległość od osi obrotu. Związane z tą siłą tzw. przyspieszenie Coriolisa jest dane wzorem $\vec{a}_C = -2(\vec{\omega} \times \vec{v})$, gdzie $\vec{\omega}$ jest wektorem prędkości kątowej charakteryzującej obrót, a \vec{v} prędkością obiektu. Przyspieszenie to jest prostopadłe zarówno do prędkości \vec{v} , jak i prędkości kątowej $\vec{\omega}$. W rozważanym na rysunku 1 przypadku w czasie wznoszenia piłki jest ono skierowane w prawo i dlatego tor lotu w fazie wznoszenia odchyła się w prawo. W fazie opadania prędkość ma przeciwny zwrot i siła Coriolisa działa w lewo, odchylając w lewo tor lotu, wskutek czego piłka uderza w powierzchnię pionowo, ale w innym miejscu.

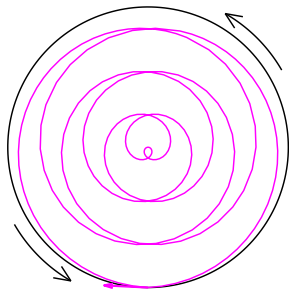
Inne, równoważne wyjaśnienie tego efektu otrzymamy, opisując lot w inercjalnym, czyli nieobracającym się układzie odniesienia – tak jakby opisał go swobodnie poruszający się astronauta przebywający na zewnątrz stacji kosmicznej. Z punktu widzenia inercjalnego obserwatora w chwili, kiedy wypuszczamy piłkę z ręki, zaczyna ona poruszać się ruchem jednostajnym prostoliniowym, ponieważ nie działają na nią żadne siły (pomijamy tutaj opory powietrza). Piłka leci więc po prostej z punktu S do punktu K , jak na rysunku 2. Prędkość początkowa piłki mierzona w układzie inercjalnym jest sumą składowej pionowej, z jaką została wyrzucona i prędkości, z jaką obraca się walec, która w punkcie S jest skierowana poziomo. Na rysunku 2 składowe te akurat są równe i piłka startuje pod kątem 45° . Dla walca o średnicy $R = 50$ m oznacza to nadanie piłce prędkości pionowej około $v \approx 22 \frac{\text{m}}{\text{s}}$. Zawodowi baseballiści potrafią miotać dwa razy szybciej, nie mówiąc o piłkarzach kopiących piłkę, natomiast prędkość rzędu $10 \frac{\text{m}}{\text{s}}$ jest osiągalna praktycznie dla każdego – tyle potrzeba, żeby podrzucić piłkę na wysokość około 5 m. Wypadkowa prędkość piłki jest większa od prędkości obrotowej walca i w czasie, kiedy piłka przeleci z punktu S do punktu K , walec obróci się zaledwie o tyle, że punkt S przesunie się do miejsca oznaczonego S' .



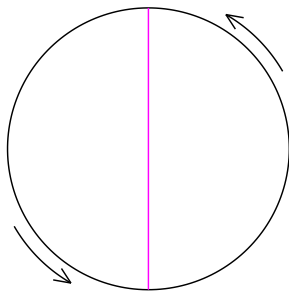
Rys. 7



Rys. 8



Rys. 9



Rys. 10

To jak mamy podrzucić piłkę, żeby wróciła do miejsca wyrzutu i dała się znowu złapać? Wystarczy nadać jej odpowiednio mniejszą prędkość początkową w układzie inercyjnym, tak aby w czasie lotu wałek zdążył się obrócić i aby punkt S' znalazł się w miejscu lądowania piłki, jak na rysunku 3. Piłka leci tu po tym samym torze co na rysunku 2, tylko wolniej – obie składowe prędkości początkowej są mniejsze. Oznacza to, że opisując ten ruch w układzie obracającym się, musimy nadać piłce prędkość początkową, która będzie miała składową w kierunku poziomym, zwróconą przeciwnie do kierunku obrotu walca, czyli rzucić ją na ukos, jak na rysunku 4. Piłka zatoczy wtedy przedstawioną na rysunku pętlę i wpadnie nam z powrotem w ręce. Maksymalna wysokość, na którą piłka się wzniesie, jest równa strzałce łuku łączącego punkty S i S' na rysunku 3, czyli odległości od punktu M do okręgu.

Łatwo się przekonać, że im wyżej piłkę chcemy podrzucić, tym bardziej ukośnie musimy to zrobić, co widać na rysunku 5 przedstawiającym torzy lotu piłek wznoszących się na różne wysokości. Rysunek 6 przedstawia te same rzuty widziane w układzie inercyjnym. Widać, że im wyżej chcemy podrzucić, tym mniejsza musi być prędkość początkowa w układzie inercyjnym, tak aby w czasie lotu wałek zdążył się jak najwięcej obrócić, a piłka pozostawała jak najdłużej w powietrzu. Najwyższa trajektoria na rysunku 5 odpowiada obrotowi walca o $\frac{3}{4}$ jego obwodu, co łatwo odczytać z rysunku 6. Nic nie stoi jednak na przeszkodzie, abyśmy tak podrzucili piłkę, aby w czasie jej lotu wałek wykonał, na przykład, półtora obrotu. Taką sytuację przedstawia rysunek 7. Na kolejnych rysunkach przedstawiono trajektorie piłki lecącej wystarczająco wolno, aby wałek wykonał dwa i pół (rys. 8) albo nawet sześć i pół obrotu (rys. 9). W układzie inercyjnym wszystkie te trzy trajektorie wyglądają w sposób przedstawiony na rysunku 10, przebiegane są tylko z różnymi prędkościami.

Widzimy, że planując rzut tak, aby móc wyrzuconą piłkę złapać, musimy uwzględnić prędkość obrotową walca i wiedzieć, jak względem kierunku tej prędkości jesteśmy zorientowani. Jasne jest, że planując rzut tak, aby trafić w jakiś konkretny punkt, niekoniecznie ten, z którego wyrzucamy, musimy zawsze uwzględnić siłę Coriolisa, która będzie zależać od tego, w którą stronę rzucamy czy kopniemy piłkę. Wewnątrz walca o małym promieniu piłka bardzo mocno kopnięta w jedną stronę błyskawicznie spadnie na ziemię, podczas gdy tak samo kopnięta w drugą może wzniesie się na niebotyczną wysokość, zataczając po drodze kilka pętli, jak na rysunku 9. Efekt ten uczyni tego typu gry znacznie trudniejsze niż w ziemskim polu grawitacyjnym.

Opisane efekty są tym mniejsze, im większy jest promień stacji R , ponieważ prędkość kątowna obrotu $\omega = \sqrt{\frac{g}{R}}$ maleje ze wzrostem promienia, a z nią maleje siła Coriolisa. Można więc minimalizować niepożądane efekty, zwiększając rozmiar stacji, ale całkowicie efektu nie da się wyeliminować, a problem z rzucaniem piłki nie będzie jedynym problemem z tego typu sztuczną grawitacją. Oprócz tego, że trzeba będzie uważać na dziwnie latające przedmioty, którym ktoś przez przypadek nadał nieodpowiednią prędkość początkową, zaobserwujemy inne ciekawe efekty. Biegając lub jeżdżąc na rowerze wewnątrz takiej stacji kosmicznej, będziemy zmieniać odczuwaną siłę ciężenia w zależności od tego, czy nasza prędkość względem stacji będzie się dodawać czy odejmować od prędkości obrotowej. Wewnątrz walca o wystarczająco małym promieniu można będzie, rozpędzając się na rowerze, oderwać się od powierzchni i doświadczyć stanu nieważkości. Trzeba też będzie uważać przy wstawianiu, bo siła Coriolisa będzie chciała nas przewrócić, tak jak zakrzywia tor wznoszącej się piłki. Trzeba będzie wstawać powoli i pochyłać się w odpowiednią stronę. W dodatku siła ciężenia, działająca na głowę, będzie mniejsza niż działająca na stopy, strumień wody lecącej z kranu będzie się zakrzywiał, podobnie jak tory spadających swobodnie przedmiotów. Powierzchnia wody w basenie będzie wklęsła, a pływanie w jedną stronę będzie trudniejsze niż w drugą. Gdy położymy ołówek na płaskim biurku, to w pobliżu lewej krawędzi będzie się staczał na lewo, a w pobliżu prawej na prawo (pod warunkiem, że kierunek lewa-prawa odpowiada kierunkowi obrotu walca). Zachęcamy Czytelników do zastanowienia się, jakie jeszcze ciekawe zjawiska będzie można zaobserwować.



Rozwiązanie zadania F 957.

Jeżeli noga piłkarza w momencie zderzenia z piłką porusza się z prędkością u , to w związanym z nią układzie odniesienia prędkość piłki wynosi $v + u$ (przyjmujemy, że oś ruchu jest zgodna z kierunkiem ruchu piłki). Po całkowicie sprężystym zderzeniu prędkość piłki w tym samym układzie odniesienia wyniesie $-(v + u)$, a jej prędkość względem ziemi wyniesie $-(v + u) - u$. Jeżeli piłka po uderzeniu zatrzyma się to $v + 2u = 0$, a stąd $u = -v/2 = -5 \text{ m/s}$. Znak minus wskazuje, że noga piłkarza powinna poruszać się w tym samym kierunku, co piłka przed uderzeniem.