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.

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 potęgowo* (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.

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

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 kilkukrotnie lądowali na Księżycu. Z kolei najdłuższe pobyty w przestrzeni kosmicznej były udziałem załóg stacji kosmicznych krążących na niskiej orbicie okołoziemskiej (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 ciążenia, a raczej jego braku. Długie pozostawanie w stanie nieważkości ma dla organizmu ludzkiego różne, bardzo negatywne skutki zdrowotne. Dlatego wizjonerzy planujący długie podróże