**Zadania RA 2019 (**obsadené **/** voľné)

1. **Aritmetika modulo p^n, t.j. určenie polynómu rozšírenia poľa, potom súčet, súčin, inverzia.**
* **Střelec + Jakabovič**
1. Aritmetika modulo 2^n, t.j. určenie polynómu rozšírenia poľa, potom súčet, súčin, inverzia.
* Hurtiš +
1. **Faktorizácia polynómov modulo p**
* **Tomšík + Zakhariás**
1. **Faktorizácia polynómov modulo 2**
* **Benčo + Šimko**
1. **Faktorizácia polynómov modulo p^n**
* **Kučerák + Košarník**
1. **Faktorizácia polynómov modulo 2^n**
* **Špes + Arendáč**
1. **Faktorizácia x^n-1 mod p**
* **Komiňák + Morávek**
1. **Faktorizácia x^n-1 mod 2**
* **Sivčák + Baláž**
1. **Určenie lineárnej zložitosti postupnosti mod 2**
* **Leščinská + Konkoľová**
1. **Určenie lineárnej zložitosti postupnosti mod p**
* **Furtkevič + Ňaňko**
1. **Určenie sférickej zložitosti rádu 1 postupnosti mod 2**
* **Debnár + Kovač + Lacza**
1. **Určenie sférickej zložitosti rádu 1 postupnosti mod p**
* **Novák + Pinteš + Dermek**
1. **Určenie sférickej zložitosti rádu 2 postupnosti mod 2**
* **Orth + Okša + Pavláková**
1. **Určenie sférickej zložitosti rádu 2 postupnosti mod p**
* **Vaškovičová + Šuhajdová + Vajdová**
1. Určenie sférickej zložitosti rádu n postupnosti mod 2
* Sikora +
1. **Nájdenie distribúcie lineárnej zložitosti modulo 2 pre dané n**
* **Šantavý + Ohyr + Yanyshevskyi**
1. Nájdenie distribúcie lineárnej zložitosti modulo p pre dané n
2. Nájdenie distribúcie sférickej zložitosti rádu 1 postupnosti mod 2 pre dané n
3. **Nájdite riešenia eliptickej krivky y^2=x^3+ax+b, mod p**
* **Cíferský + Gál**
1. Nájdite riešenia eliptickej krivky y^2=x^3+ax+b, mod p a vygenerujte tabuľku pre súčty