

ეილერის მახასიათებლის გამოთვლა

ალექსანდრე ლომაძე

alexandre.lomadze024@ens.tsu.edu.ge

ნაშრომი ეხება ალგებრული ამოცანის კომპიუტერულად გადაჭრის საკითხს. კერძოდ, მორავას K-თეორიის ჯგუფების ბაზისის ელემენტების რაოდენობის გამოთვლას ანუ მისი რანგის დადგენას. ნაშრომი ეყრდნობა პროგრამას, რომელიც გამოყენებული მქონდა სამაგისტრო ნაშრომში. ანუ იყენებს P ჯგუფების აბელური ქვეჯგუფების აღწერას (მათ კლასიფიკაციას, რაოდენობას და ა.შ.).

კერძოდ ნაშრომში გადაჭრილია ეილერის მახასიათებლის (*) კომპიუტერულად გამოთვლის საკითხი. ეს ფორმულა გამოთვლილია ყველა 32 რიგის ჯგუფისთვის და ასევე სხვადასხვა სპეციფიკური მაღალი რიგის ჯგუფისათვის. ჩემ მიერ წარმოდგენილი პროგრამა ამ ფორმულას გამოითვლის თითქმის ნებისმიერი სიდიდის ჯგუფისთვის, მაგრამ 1024 ან ნაკლებ ელემენტისანი ჯგუფებისთვის უფრო პრაქტიკული გამოსაყენებელია რადგან ჯგუფის ელემენტების რაოდენობასთან ერთად იზრდება მისი აბელური ქვეჯგუფების რაოდენობა, და შესაბამისად იზრდება კომპილაციის დროც).

ეილერის მახასიათებელი:

$$\chi_{n,p}(G) = \sum_{A \in G} \frac{|A|}{|G|} * \mu(A) * \chi(A) \quad (*)$$

ამ ნაშრომის გამოყენება და განვრცობა შესაძლებელია რამოდენიმე მიმართულებით, ალგებრაში ამ ფორმულის მარტივად გამოთვლა შეიძლება გამოვიყენოთ კონკრეტული ჰიპოტეზის განმტკიცებაში, ხოლო შემდგომ, ამის საფუძველზე, შესაძლებელი იქნება გარკვეული კრიპტოსისტემის აგებაც.