Using decomposition groups to prove theorems about quadratic residues

Perutka, Tomáš[1]

This paper introduces new proofs of some theorems about quadratic residues via decomposition groups and Frobenius automorphisms. What does it mean, though? The quadratic residues are quite important objects in number theory with many applications, both theoretical (solving quadratic congruences) and practical ones (in coding theory, acoustics etc.). Consider an odd prime p – that is, a natural number which is divisible only by 1 and itself (e.g. 3,5,11,...). We say that an integer a, which is not divisible by p, is a *quadratic residue modulo p* if its remainder after dividing by p is the same as the remainder of some perfect square (ie. c^2 where c is an integer). For example: -1 is a quadratic residue modulo 5 since it has the same remainder after dividing by 5 as $4 = 2^2$; 10 is a quadratic residue modulo 13 since it has the same remainder as $36 = 6^2$.

However, the quadratic residues and their properties are not the main focus of the paper, *the proofs* of the properties are. The most important tool used throughout the proofs is the *Frobenius automorphism*, a somewhat abstract and difficult concept from number theory. Its study has led to many breakthroughs, for example, to the proof of Fermat's Last Theorem. Therefore, it is not easy to explain the concept in short, however, let us attempt to do so.

We know that each integer can be decomposed uniquely into a product of prime numbers and the prime numbers cannot be decomposed any further (only as $1 \cdot p$ which is not interesting). However, this is no longer true if we move on to some larger set of numbers. For example, consider the set $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}; a, b \text{ are the integers}\}$.

In this set, we obtain $7 = (3 + \sqrt{2})(3 - \sqrt{2})$, so we have just non-trivially decomposed a prime. This leads to a question: considering a set $\mathcal{O}$ similar as $\mathbb{Z}[\sqrt{2}]$ above (more specifically: the ring of integers of some finite field extension of the field of rational numbers), what can be said about how a prime p can be decomposed? This question has been one of the main questions in number theory for a long time. Frobenius automorphism of a prime p offers a partial answer. For any prime p and "a sufficiently nice" set $\mathcal{O}$, we always have a function $Frob_{p,\mathcal{O}}: \mathcal{O} \to \mathcal{O}$. Once the function is known, we know how p decomposes in $\mathcal{O}$. In particular, if $Frob_{p,\mathcal{O}}$ is an identity, p decomposes as much as possible. But how does all of this relate to the quadratic residues? Surprisingly, it can be shown that in the case $\mathcal{O} = \mathbb{Z}[\sqrt{d}]$, where $d \neq 0, 1$ is an integer , we get for any prime $p \neq 2$ the following: **$Frob_{p,\mathcal{O}}$ is an identity if and only if d is a quadratic residue modulo p.** We can then prove many marvelous theorems with this information and you can find out how in the paper.

Tomáš Perutka *is a student at the Faculty of Science in Masaryk University, Brno. He studies Pure Mathematics in the Department of Mathematics and Statistics. He is now mostly interested in algebraic number theory, category theory, and sheaf-theoretical methods in geometry and topology. He has been interested in number theory since high school; he has written there two manucripts about it which both competed in the competition SOČ. The first one won the first place in the competition and it also won an award from the Learned Society of the Czech Republic. Moreover, Tomas Perutka obtained an award "České hlavičky" and it was chosen to represent the Czech Republic at the international competition CASTIC in Macao where it won the bronze medal. The time Tomáš does not spend with mathematics he usually spends doing ballroom dancing or practising kung-fu.*

1 *Faculty of Science, Masaryk University, 611 37 Brno, Czechia*