Arithmetic and Algebraic Methods for Solving Multiplicative Quadratic Congruences

Sukhotin, Dmitry (School: Higher School of Economics Lyceum)

Research question: How the quadratic congruence could be solved using methods of modular arithmetic and group theory? Procedures used: An algebraic method for confirming the existence of any solutions was demonstrated at the beginning of the study. As a result, some necessary conditions for the solutions to exist were obtained. The first step: solving the given congruence as a quadratic equation using a p-adic version of the Newton method, where we increase the power of p, approximating the value of x with respect to p-adic absolute value. Group theory approach also leads to solving a linear equation, but in a completely different way. It involves constructing an isomorphism, which assigns every element of the initial multiplicative group modulo 10^n to an element of the additive group. One more method (devised in this research) involves algebraic transformations, making the original congruence linear. It is based on adding odd numbers to form the square, satisfying the congruence and finding the sum of these numbers. Final step: a generalization of the initial problem. It raised a question about the existence of squares that contain the number a inside, which means that there is at least one digit on the right of the last digit of a in the square. Solution of this problem is the most important result of this study. Results: necessary and sufficient conditions for solvability of a quadratic congruence were found, the existence of a square containing any chosen number was proven.

Awards Won: