Title: Solving diophantine equations by factorization in number fields

Author: Bc. Maroš Hrnčiar

Department: Department of Algebra

Supervisor: Mgr. Vítězslav Kala, Ph.D., Mathematical Institute, University of Göttingen

Abstract: The question of solvability of diophantine equations is one of the oldest mathematical problems in the history of mankind. While different approaches have been developed for solving certain types of equations, this thesis predominantly deals with the method of factorization over algebraic number fields. The idea behind this method is to express the equation in the form $L = y^n$ where $L$ equals a product of typically linear factors with coefficients in a particular number field. Provided that several assumptions are met, it follows that each of the factors must be the $n$–th power of an element of the field. The structure of number fields plays a key role in the application of this method, hence a crucial part of the thesis presents an overview of algebraic number theory. In addition to the general theoretical part, the thesis contains all the necessary computations in specific quadratic and cubic number fields describing their basic characteristics. However, the main objective of this thesis is solving specific examples of equations. For instance, in the case of equation $x^2 + y^2 = z^3$ we focus on dealing with common factors in the ring of integers, while in the equation $x^3 + 2x + 1 = y^2$ problems occur with factorization over the cubic field itself. When considering the equation $x^2 - 2 = y^3$ and the field $\mathbb{Q}(\sqrt{2})$ it is more complicated to determine a unit group which relies on solutions of Pell’s equation. Extensive calculations are needed to describe the class group of the field related to the equation $x^2 - 79 = y^3$. Using the method of factorization over number fields we are usually able to reduce the given diophantine equation to several Thue equations and despite the fact that the latter are often not elementarily solvable, the generally known effective algorithm may be applied. Finally we prove number of statements regarding the equation $x^2 - dc^2 = y^n$ in $p$–adic numbers.

Keywords: diophantine equation, factorization, number field, class group, unit group