JASB
JOURNAL OF THE ASB SOCIETY

Solving Diophantine Equations by Factoring in Number Fields

Pezlar, Zdeněk[1]*

1 *Gymnázium Brno, třída Kapitána Jaroše 14, příspěvková organizace*

About the author

Zdeněk Pezlar is a student at the třída Kaptiána Jaroše grammar school, Brno. At the moment he is mostly interested in olympiad mathematics and next to that in number theoretic properties of elliptic curves. He has so far written two projects which have both competed in the Student Professional Activities - SPA (Středoškolská odborná činnost - SOC) competition. The first one won first place in the competition, an award from the Learned Society of the Czech Republic and a special prize at the international competition EUCYS. The second project placed third at the competition and won the "České hlavičky" award. Apart from SOČ, Zdeněk has represented the Czech Republic in olympiad mathematics - he has won a bronze and a silver medal at the Middle European olympiad MEMO. In the time he does not spend with mathematics, he often plays the piano and also plays frisbee

Explanation for general audience

The article focuses on a branch of mathematics called 'algebraic number theory' and in particular its applications in elementary number theory - solving hard diophnatine equations. Let's back up a bit.

When working with integers, we often make use of either modular arithmetic or their unique factorisation into primes. The crown jewels of modular arithmetic are quadratic residues, which allow for more advanced discussions concerning divisibility over the integers. Theorems such as Euler's criterion then allow us to quickly decide when a given diophantine equation has no integer solutions - simply find a modulus under which no solutions exist. These basic methods can, however, get us only so far. Take an equation such as $x^2 + 13 = y^3$ for an example. It has an integral solution for $x = 70$, so a solution modulo every integer, and no obvious way to factor presents itself. So how do we proceed? Well, it is not entirely true, that no easy factorisation exists, over the complex numbers one is immediate: $x^2 + 13 = (x + \sqrt{(}-13))(x - \sqrt{(}-13))$. What use could that be to us, though?

Questions such as that puzzled the old masters. When attempting to solve the famous Fermat's Last Theorem - i.e showing that the equation $x^n + y^n = z^n$ has no non-trivial integral solutions for $n > 2$ - mathematicians such as Carl Friedrich Gauss, Ernst Kummer and Peter Gustav Dirichlet pioneered the field of algebraic number theory and paved the way for mathematicians in centuries to come. In particular they tried considering number theoretic of complex roots of polynomials over the integers, or rather extensions of $\mathbb{Q}$ containing these numbers. It turns out that studying the ideals in certain subrings of these number fields is the way to proceed. Indeed, it is true, that ideals uniquely decompose into prime ideals, much like ordinary integers do. This is in stark contrast with the rings themselves, which mostly do not admit unique factorisation. In what is a beautiful connection of those two concepts, we introduce the ideal class group, which neatly connects both concepts and provides the final piece of the puzzle allowing us to solve equations by factoring in fields containing, say, the square-root of -13.