Reg. No: 2017/27/N/ST1/00497; Principal Investigator: mgr Jędrzej Garnek

Abelian varieties over p-adic fields
DESCRIPTION FOR THE GENERAL PUBLIC

Jędrzej Garnek

Recall that an *algebraic variety* is a set defined by polynomial equations with coefficients in a given field K. An *abelian variety* is a projective algebraic variety, such that the set of its points forms a group with a group law given by some rational functions. The first mathematician to consider elliptic curves (one dimensional abelian varieties) was probably Diophantus, who invented a method of "doubling" points on them. Elliptic curves and Jacobians of higher genus curves appeared also in the theory of complex functions, developed by nineteenth century mathematicians. The next big step in this theory was the problem posed by Henri Poincaré: *if E is an elliptic curve defined over $\mathbb{Q}$, is the abelian group $E(\mathbb{Q})$ finitely generated?* This was answered positively by Louis Mordell in 1922. This initiated the study of elliptic curves and abelian varieties defined over number fields. The next years brought a systematic development of the theory of abelian varieties over number fields. We mention only the work of Wiles, which ultimately led to proving the Fermat's Last Theorem in 1994.

Suppose that A is an abelian variety of dimension g over a field K. The *n-torsion subgroup of A* is the set of points that become zero after repeatedly adding them n times. We know many properties of the n-torsion. For example, we know that usually there are n^{2g} n-torsion points on a variety of dimension g. However, the "algebraic" properties of the n-torsion (concerning the "rationality" of the coefficients of torsion) are much harder to describe. The general philosophy is that the torsion is usually *as complex as it can be* for big n.

Recall that every integer has a binary expansion in the form of a sum of powers of two. If we allow numbers with an infinite binary expansion, we obtain *the field of 2-adic numbers*, $\mathbb{Q}_2$. This is achieved by interpreting high powers of 2 as being very "small". Similarly, for each prime p one can consider the field of p-adic numbers, $\mathbb{Q}_p$. The concept of p-adic numbers was motivated primarily by an attempt to bring the techniques of calculus (the theory of power series) into number theory.

The *local torsion* of an abelian variety $A/\mathbb{Q}$ is its p-torsion over the field $\mathbb{Q}_p$. A folklore conjecture states that for a "typical" elliptic curve over $\mathbb{Q}$ its local torsion should vanish for almost all primes p. This conjecture may be generalized using the notion of the p-degree: a quantity that measures the least complexity of a non-zero p-torsion point. For a "typical" elliptic curve the p-degree should be large, as p tends to infinity. The primary motivation for this kind of problems is the theory of deformations of Galois representations. The goal of the first part of the project is to describe the properties of the p-degree of an abelian varieties $A/\mathbb{Q}_p$.

We expect also to find a different application of local torsion of abelian varieties. The *nth division field K_n* of an abelian variety $A/\mathbb{Q}$ is obtained by adjoining to $\mathbb{Q}$ the coordinates of its n-torsion points. The *class number* of K_n measures to which extent the unique factorisation in K_n fails. We predict that class numbers of the division fields might be estimated in terms of invariants involving the local torsion of A.

The second part of this project focuses on the notion of the *canonical lift* of an abelian variety. An abelian variety given by polynomial equations with coefficients in some finite field may be "lifted" to a p-adic field in many ways, but there is one *canonical way*, preserving some nice properties. Canonical lifts have a broad scope of applications in algorithmic algebraic number theory. They are used among other things for counting points on elliptic curves over finite fields, constructing elliptic curves over finite fields with a prescribed number of points, computing Hilbert class polynomials and constructing hyperelliptic curves suitable for cryptology. We plan to find a connection between canonical lifts and the p-degree conjecture. Also, we plan to focus on canonical lifts of higher dimensional abelian varieties.