PETR LISONEK, Simon Fraser University

Identities for Kloosterman sums

Kloosterman sums are exponential sums defined on finite fields that are important in Cryptography and Coding Theory. As a motivation example we mention an application in the construction of pseudo-random sequences that are used as key streams in stream ciphers. Identities relating values of Kloosterman sums are thus of interest. We use the theory of elliptic curves to show that an infinite family of such identities can be obtained from the classical modular polynomials. We show that some identities that have been proved earlier by other authors arise as special cases of our result.