**Nesterenko, A. Yu.**

**Constructions of elliptic curves endomorphisms.** (English) Zbl 07397100


Summary: Let \( k \) be an imaginary quadratic field. Consider an elliptic curve \( E(F_p) \) defined over prime field \( F_p \) with given ring of endomorphisms \( o_K \), where \( o_K \) is an order in a ring of integers \( Z_k \).

An algorithm permitting to construct endomorphism of the curve \( E(F_p) \) corresponding to the complex number \( \tau \in o_K \) is presented. The endomorphism is represented as a pair of rational functions with coefficients in \( F_p \). To construct these functions we use continued fraction expansion for values of Weierstrass function. After that we reduce the rational functions modulo prime ideal in finite extension of \( K \). One can use such endomorphism for elliptic curve point exponentiation.

**MSC:**

- 94A60 Cryptography
- 14G50 Applications to coding theory and cryptography of arithmetic geometry
- 11T71 Algebraic coding theory; cryptography (number-theoretic aspects)

**Keywords:**

- elliptic curve;
- continued fraction expansion;
- reduction modulo prime ideal;
- point exponentiation

**Full Text:** DOI MNR

**References:**


This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.