Journal de Théorie des Nombres
de Bordeaux **16** (2004), 555–568

Constructing elliptic curves over finite fields using double eta-quotients

par Andreas ENGE et Reinhard SCHERTZ

Résumé. Nous examinons une classe de fonctions modulaires pour $\Gamma^0(N)$ dont les valeurs engendrent des corps de classes d'anneaux d'ordres quadratiques imaginaires. Nous nous en servons pour développer un nouvel algorithme de construction de courbes elliptiques à multiplication complexe. Vu que le genre des $X_0(N)$ associées n'est pas zéro, le calcul de la courbe se fait à l'aide de certains polynômes modulaires.

Étant un produit de quatre fonctions η, les fonctions modulaires proposées peuvent être vues comme une généralisation naturelle des fonctions traitées par Weber et généralement utilisées pour construire des courbes elliptiques à multiplication complexes. Contrairement au cas des fonctions de Weber, les valeurs des fonctions examinées ici engendrent tous les corps de classes d'anneaux de n'importe quel ordre quadratique imaginaire sans tenir compte des congruences satisfaites par leur discriminant modulo des puissances de 2 ou 3.

Abstract. We examine a class of modular functions for $\Gamma^0(N)$ whose values generate ring class fields of imaginary quadratic orders. This fact leads to a new algorithm for constructing elliptic curves with complex multiplication. The difficulties arising when the genus of $X_0(N)$ is not zero are overcome by computing certain modular polynomials.

Being a product of four η-functions, the proposed modular functions can be viewed as a natural generalisation of the functions examined by Weber and usually employed to construct CM-curves. Unlike the Weber functions, the values of the examined functions generate any ring class field of an imaginary quadratic order regardless of the congruences modulo powers of 2 and 3 satisfied by the discriminant.

Andreas Enge
INRIA Futurs & LIX (CNRS/UMR 7161)

Manuscrit reçu le 8 avril 2003.

École polytechnique
91128 Palaiseau cedex, France
E-mail : enge@lix.polytechnique.fr
URL: http://www.lix.polytechnique.fr/Labo/Andreas.Enge/

Reinhard Schertz
Institut für Mathematik
Universität Augsburg
86135 Augsburg, Deutschland
E-mail : schertz@math.uni-augsburg.de