Journal de Théorie des Nombres
de Bordeaux **19** (2007), 663–681

Computing the cardinality of CM elliptic curves using torsion points

par François MORAIN*

Résumé. Soit $\mathcal{E}/\overline{\mathbb{Q}}$ une courbe elliptique avec multiplications complexes par un ordre d'un corps quadratique imaginaire $\mathbf{K}$. Le corps de définition de $\mathcal{E}$ est le corps de classe de rayon Ω associé à l'ordre. Si le nombre premier p est scindé dans Ω, on peut réduire $\mathcal{E}$ modulo un des facteurs de p et obtenir une courbe E définie sur $\mathbb{F}_p$. La trace du Frobenius de E est connue au signe près et nous cherchons à déterminer ce signe de la manière la plus rapide possible, avec comme application l'algorithme de primalité ECPP. Dans ce but, nous expliquons comment utiliser l'action du Frobenius sur des points de torsion d'ordre petit obtenus à partir d'invariants de classes qui généralisent les fonctions de Weber.

Abstract. Let $\mathcal{E}/\overline{\mathbb{Q}}$ be an elliptic curve having complex multiplication by a given quadratic order of an imaginary quadratic field $\mathbf{K}$. The field of definition of $\mathcal{E}$ is the ring class field Ω of the order. If the prime p splits completely in Ω, then we can reduce $\mathcal{E}$ modulo one the factors of p and get a curve E defined over $\mathbb{F}_p$. The trace of the Frobenius of E is known up to sign and we need a fast way to find this sign, in the context of the Elliptic Curve Primality Proving algorithm (ECPP). For this purpose, we propose to use the action of the Frobenius on torsion points of small order built with class invariants generalizing the classical Weber functions.

François Morain
Laboratoire d'Informatique
de l'École polytechnique (LIX)
F-91128 Palaiseau Cedex
France
E-mail : morain@lix.polytechnique.fr
URL: http://www.lix.polytechnique.fr/Labo/Francois.Morain

Manuscrit reçu le 28 aout 2006.
Mots clefs. Elliptic curves, complex multiplication, modular curves, class invariants, ECPP algorithm, SEA algorithm.

* Projet TANC, Pôle Commun de Recherche en Informatique du Plateau de Saclay, CNRS, École polytechnique, INRIA, Université Paris-Sud. The author is on leave from the French Department of Defense, Délégation Générale pour l'Armement.