

ATELIER « COMPTAGE DE POINTS : THÉORIE, ALGORITHMES ET PRATIQUE »  
19–23 AVRIL 2010

WORKSHOP ON COUNTING POINTS: THEORY, ALGORITHMS AND PRACTICE  
APRIL 19–23, 2010

## Algebraic construction of the Elkies factor

Christiane Peters

Department of Mathematics and Computer Science  
Technische Universiteit Eindhoven  
P.O. Box 513  
5600 MB Eindhoven  
THE NETHERLANDS

c.p.peters@tue.nl

---

Let  $\ell$  be an Elkies prime. We compute a factor of degree  $(\ell - 1)/2$  of the  $\ell$ th division polynomial. The computation builds on the algebraic construction of a modular equation  $U_\ell$  as given in [1] which does not involve using modular forms. We show that the Elkies factor can be derived algebraically—again without using modular forms—as the greatest common divisor of the  $\ell$ th division polynomial and a polynomial depending on a zero of  $U_\ell$  in  $\mathbf{F}_q$ .

This result is part of my diploma thesis written under supervision of Peter Bürgisser and Preda Mihăilescu.

Reference :

[1] L. S. Charlap, R. Coley, and D. P. Robbins, *Enumeration of rational points on elliptic curves over finite fields*, Draft 1991.