Cryptology ePrint Archive: Report 2011/666

A Gross-Zagier formula for quaternion algebras over totally real fields

Eyal Z. Goren and Kristin E. Lauter

Abstract: We prove a higher dimensional generalization of Gross and Zagier's theorem on the factorization of differences of singular moduli. Their result is proved by giving a counting formula for the number of isomorphisms between elliptic curves with complex multiplication by two different imaginary quadratic fields K and $K^\prime$, when the curves are reduced modulo a supersingular prime and its powers. Equivalently, the Gross-Zagier formula counts optimal embeddings of the ring of integers of an imaginary quadratic field into particular maximal orders in $B_{p, \infty}$, the definite quaternion algebra over $\mathbb {Q}$ ramified only at p and infinity. Our work gives an analogous counting formula for the number of simultaneous embeddings of the rings of integers of primitive CM fields into superspecial orders in definite quaternion algebras over totally real fields of strict class number 1. Our results can also be viewed as a counting formula for the number of isomorphisms modulo $\frak{p} \vert p$ between abelian varieties with CM by different fields. Our counting formula can also be used to determine which superspecial primes appear in the factorizations of differences of values of Siegel modular functions at CM points associated to two different CM fields, and to give a bound on those supersingular primes which can appear. In the special case of Jacobians of genus 2 curves, this provides information about the factorizations of numerators of Igusa invariants, and so is also relevant to the problem of constructing genus 2 curves for use in cryptography.

Category / Keywords: public-key cryptography / hyperelliptic curve cryptosystem

Publication Info: none

Date: received 8 Dec 2011

Contact author: klauter at microsoft com