Invent. math. 84, 225-320 (1986)

Inventiones mathematicae

© Springer-Verlag 1986

Heegner points and derivatives of L-series

Benedict H. Gross[1] and Don B. Zagier[2]

[1] Department of Mathematics, Brown University, Providence, RI 02912, USA
[2] Department of Mathematics, University of Maryland, College Park, MD 20742, USA and Max-Planck-Institut für Mathematik, Gottfried-Claren-Strasse 26, D-5300 Bonn 3, Federal Republic of Germany

to John Tate

Table of Contents

I. Introduction and statement of results

The main theorem of this paper gives a relation between the heights of Heegner divisor classes on the Jacobian of the modular curve $X_0(N)$ and the first derivatives at $s=1$ of the Rankin L-series of certain modular forms. In the first six sections of this chapter, we will develop enough background material on modular curves, Heegner points, heights, and L-functions to be able to state one version of this identity precisely. In § 7 we will discuss some applications to the conjecture of Birch and Swinnerton-Dyer for elliptic curves. For example, we will show that any modular elliptic curve over $\mathbb{Q}$ whose L-function has a simple zero at $s=1$ contains rational points of infinite order. Combining our work with that of Goldfeld [12], one obtains an effective lower bound for the class numbers of imaginary quadratic fields as a function of their discriminants (§ 8). In § 9 we will describe the plan of proof and the contents of the remaining chapters.

Many of the results of this paper were announced in our Comptes Rendus note [17]. A more leisurely introduction to Heegner points and Rankin L-series may be found in our earlier paper [13].

§ 1. The curve $X_0(N)$ over $\mathbb{Q}$

Let $N \geqq 1$ be an integer. The curve $X=X_0(N)$ may be informally described over $\mathbb{Q}$ as the compactification of the space of moduli of elliptic curves with a cyclic subgroup of order N. It is known to be a complete, non-singular, geometrically connected curve over $\mathbb{Q}$. Over a field k of characteristic zero, the points x of X correspond to diagrams

$$\phi: E \to E' \tag{1.1}$$

where E and E' are (generalized) elliptic curves over k and ϕ is an isogeny over k whose kernel A is isomorphic to $\mathbb{Z}/N\mathbb{Z}$ over an algebraic closure $\bar{k}$. The function field of X over $\mathbb{Q}$ is generated by the modular invariants $j(x)=j(E)$ and $j'(x)=j(E')$; these satisfy the classical modular equation of level N: $\phi_N(j,j')=0$ [2].

The cusps of X are the points where $j(x)=j'(x)=\infty$. They correspond to diagrams (1.1) between certain degenerate elliptic curves, where $A=\ker\phi$ meets each geometric component of E [7, 173ff.]. There is a unique cusp where E has 1 component and a unique cusp where E has N components; these are denoted ∞ and 0 respectively and are rational over $\mathbb{Q}$.