Journal of Number Theory 167 (2016) 31–73

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Class pairings and isogenies on elliptic curves[☆]

Duncan A. Buell, Gregory S. Call[*]

ARTICLE INFO

Article history:
Received 9 November 2015
Received in revised form 12 February 2016
Accepted 12 February 2016
Available online 19 April 2016
Communicated by David Goss

Keywords:
Elliptic curves
Ideal class pairing
Idele classes
Isogenies
Weil descent pairing

ABSTRACT

In [Bue76,Bue77] a non-trivial homomorphism δ was constructed from $\mathbb{Q}$-rational points on an elliptic curve to the ideal class group of a quadratic field $K = \mathbb{Q}(\sqrt{\mathcal{D}})$. In [MT83] it was conjectured that δ was related to a pairing on points of $E(K)$, which has come to be known as the ideal class pairing. In this paper we will show how to write the ideal class pairing in an explicit and easy-to-compute manner, and we will prove by direct calculation that the homomorphism δ is identical to the ideal class pairing with one argument fixed. For any elliptic curve E over a number field K, we will show how to extend the ideal class pairing to a full pairing on $E(K)$, called simply the elliptic curve class pairing, which maps into an extension of the idele class group of K. The explicit formulas we will derive for the elliptic curve class pairing will enable us to prove that there is a natural relationship between this pairing and the Weil descent pairing. The kernel of the elliptic curve class pairing will be determined in many cases where one argument is taken to be a fixed torsion point and, as a corollary, the kernel of δ will be computed for a class of elliptic curves over imaginary quadratic fields.

[☆] Research supported (in part) by a grant from the Amherst College Faculty Research Award Program.
[*] Corresponding author.
E-mail address: gscall@amherst.edu (G.S. Call).

http://dx.doi.org/10.1016/j.jnt.2016.02.030
0022-314X/© 2016 Elsevier Inc. All rights reserved.

1. Introduction

In [Bue76,Bue77] a non-trivial homomorphism was constructed from rational points on the elliptic curve

$$E : y^2 = 4x(x^2 + Bx + C) + \mathcal{D}$$

(where $B, C \in \mathbb{Z}$, and $\mathcal{D}$ is the discriminant of a quadratic number field) to the ideal class group of $K = \mathbb{Q}(\sqrt{\mathcal{D}})$. This homomorphism, which we denote by δ, is given by the explicit formula

$$\delta\left(\left(\frac{a}{e^2}, \frac{b}{e^3}\right)\right) = cl\left(aX^2 + bXY + (a^2 + Bae^2 + Ce^4)Y^2\right) \tag{1}$$

where $a, b, e \in \mathbb{Z}$ with $\gcd(a, e) = 1$ and $\gcd(b, e) \leq 2$, and cl denotes the class of the quadratic form. The resulting quadratic form has discriminant $e^6\mathcal{D}$. When we use the standard homomorphism from the classes of quadratic forms to ideal classes, we get an ideal class in $\mathbb{Q}(\sqrt{\mathcal{D}})$. The homomorphism δ explains various explicit constructions of non-trivial Sylow subgroups in ideal classes of quadratic fields. See Section 5 for details.

In [MT83] it was conjectured that δ was related to a pairing on points of $E(K)$, which has come to be known as the *ideal class pairing*. This conjecture was proven in [Cal86]. In particular, it was shown how to express this pairing in terms related to the Néron local height pairings associated to the primes $\mathfrak{p}$ of K. The original construction of δ had the virtue of being explicit and easy to compute, though it had certain limitations. In this paper we shall demonstrate how to write the ideal class pairing in a similarly explicit and easy-to-compute manner. In particular, we will show by direct calculation that the homomorphism δ is the ideal class pairing with one argument fixed (see Theorem 3.14), and thus provide another proof of the first author's theorem that δ is a homomorphism.

Among the limitations of the original definition of δ are that it depends on the particular equation chosen for the curve E and it was only defined for curves defined over quadratic number fields. The ideal class pairing, on the other hand, depends only on the isomorphism class of E/K and is defined for elliptic curves over arbitrary number fields. Despite these improvements, the ideal class pairing is not without its own limitations which prompt us to extend its definition in two important ways. Suppose now that E is an elliptic curve over an arbitrary number field K. We will recall in Section 2.1 that the ideal class pairing is defined only for *good reduction pairs* $(P, Q) \in E(K)$. By considering the Néron local pairings associated to the archimedean valuations of K we will extend the pairing to a map into the idele class group of K, which we call the *idele class pairing*. As a final step, we'll eliminate the restriction to good reduction pairs and show that we can still define a pairing into an extension of the idele class group of K, which we'll call simply the *elliptic curve class pairing*.