Journal of Number Theory 161 (2016) 119–134

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

# On 3-adic heights on elliptic curves

Jennifer S. Balakrishnan

*Mathematical Institute, University of Oxford, Woodstock Road, Oxford OX2 6GG, UK*

A R T I C L E I N F O

*Article history:*
Received 19 October 2014
Received in revised form 30 May 2015
Accepted 31 July 2015
Available online 4 August 2015
Communicated by Jerome Hoffman, Robert Perlis, Ling Long, Karl Mahlburg, Jorge Morales, Holly Swisher

*MSC:*
11G50
11Y40

*Keywords:*
$p$-adic heights
Kedlaya's algorithm
Elliptic curves
$p$-adic Birch and Swinnerton-Dyer conjecture

A B S T R A C T

In 2006, Mazur, Stein, and Tate [5] gave an algorithm for computing $p$-adic heights on elliptic curves over $\mathbb{Q}$ for good, ordinary primes $p \geq 5$. In this paper, we extend their algorithm to the case of $p = 3$. We also discuss the 3-adic precision that must be maintained throughout the computation, following the work of Harvey [2]. We conclude by giving examples of 3-adic regulators and their compatibility with the 3-adic Birch and Swinnerton-Dyer conjecture, computed using Sage [9].


## 1. Introduction

In 2006, Mazur, Stein, and Tate [5] gave an algorithm to compute the cyclotomic $p$-adic height of a rational point on an elliptic curve $E$ over $\mathbb{Q}$, assuming that $p \geq 5$ is a prime of good, ordinary reduction. This height plays a key role in the statement

*E-mail address:* balakrishnan@maths.ox.ac.uk.

http://dx.doi.org/10.1016/j.jnt.2015.07.003
0022-314X/

of the $p$-adic Birch and Swinnerton-Dyer conjecture, where the $p$-adic regulator is the determinant of a matrix of $p$-adic height pairings on the free part of the Mordell–Weil group.

The work of Mazur, Stein, and Tate uses an interpretation of the $p$-adic sigma function as the solution to a certain $p$-adic differential equation, which involves a constant given by a special value of the weight two Eisenstein series $\mathbf{E}_2$. One of their key observations was that this constant could be computed very quickly in terms of the action of Frobenius on $H^1_{\mathrm{dR}}(E)$, the first de Rham cohomology group of $E$, by using Kedlaya's algorithm [4]. More recently, Harvey [2] showed that the linear dependence on $p$ in Kedlaya's algorithm could be reduced to $\sqrt{p}$, and in turn, gave a faster algorithm to compute $p$-adic heights, along with bounds on $p$-adic precision necessary to ensure that the algorithm produced a certain number of provably correct $p$-adic digits.

These algorithms use Kedlaya's algorithm by working with the basis $\left\{\frac{dx}{y}, x\,\frac{dx}{y}\right\}$ of $H^1_{\mathrm{dR}}(E)$, with $E$ given by a "short" Weierstrass model $y^2 = x^3 + ax + b$. To use Kedlaya's algorithm, the given model of the curve must be smooth at $p$, which potentially presents an obstruction to the method of Mazur, Stein, and Tate and Harvey at the prime $p = 3$.

However, Kedlaya's algorithm was originally formulated in greater generality and can be applied, for primes $p > 2$, to hyperelliptic curves over $\mathbb{Q}$ of the form $y^2 = f(x)$, where $\overline{f}(x) \in \mathbb{F}_p[x]$ has distinct roots modulo $p$. Our strategy to compute 3-adic heights makes use of this and takes as input a more general model of the elliptic curve to carry out Kedlaya's algorithm at $p = 3$. Nevertheless, since the computation of $p$-adic heights relies on a particular model of the curve and a certain basis of de Rham cohomology with respect to that model, we must account for this, which we do by performing a change of basis.

This allows us to extend the work of Harvey [2] and Mazur, Stein, and Tate [5] to the computation of 3-adic heights on elliptic curves. Nevertheless, one subtlety introduced by this method is that a quantity used to compute the special value of $\mathbf{E}_2$ is no longer guaranteed to be a $p$-adic unit. We examine its valuation and use this to formulate our bounds on $p$-adic precision.

The structure of this paper is as follows: in Section 2, we give an overview of the method of Mazur, Stein, and Tate and discuss the role of Frobenius via Kedlaya's algorithm. In Section 3, we give an explicit formula relating the Frobenius matrix on the short Weierstrass model to the Frobenius matrix on a more general model of the elliptic curve. In Section 4, we discuss the 3-adic precision that must be maintained throughout the calculation to give a certain number of correct digits in the height calculation, thereby extending a theorem of Harvey [2]; we also give an algorithm to compute 3-adic heights. Section 5 presents a selection of examples of 3-adic regulators and uses this to give examples of compatibility with the 3-adic Birch and Swinnerton-Dyer conjecture in higher rank.