Descents on Curves of Genus 1

Samir Siksek

Submitted by Samir Siksek
to the University of Exeter
as a thesis for the degree of
Doctor of Philosophy
in the Faculty of Science
July 1995

I certify that all the material in this thesis which is not my own work has been clearly identified and that no material is included for which a degree has previously been conferred upon me.

Samir Siksek

Abstract. In this thesis we improve on various methods connected with computing the Mordell-Weil group of an elliptic curve. Our work falls into several parts:

1. We give a new upper bound for the difference of the logarithmic and canonical heights of points on elliptic curves.

2. We give a new method for performing the infinite descent on an elliptic curve. This is essentially a lattice enlargement algorithm.

3. We show how to compute the 2-Selmer group of an elliptic curve defined over the rationals by a method which has complexity

$$L_D(0.5, c_1) = (e^{(\log D)^{0.5}(\log\log D)^{0.5}})^{c_1+o(1)},$$

   where $D = |\Delta|$ the absolute value of the discriminant of the elliptic curve, and c_1 is a positive constant. This part is based on joint work with N. Smart.

4. We give a recipe for 'higher descents' on homogeneous spaces arising from the 2-descent. This is useful in dealing with homogeneous spaces which are everywhere locally soluble but for which a search for points does not reveal any global points.

5. We give algorithms for checking our homogeneous spaces for solubility over completions of number fields.

Acknowledgements

I am grateful to my supervisor John Cremona for his help and encouragement and for suggesting the topic of the thesis to me. I would also like to thank EPSRC for their financial support, Robin Chapman for putting up with my questions, Ray Miller and Jeremy Bygott for help with LaTeX.

Finally I would like to thank my family for their patience and support.

Contents

1 Introduction **6**

1.1 The Mordell-Weil Theorem 7

1.1.1 The Weak Mordell-Weil Theorem 7

1.1.2 The Infinite Descent 9

1.2 Outline of the Usual Method of Computing the Mordell-Weil Group 11

1.2.1 Computing the Torsion Subgroup of $E(K)$ 11

1.2.2 Computing the 2-Selmer Group of E 12

1.2.3 Computing $E(K)/2E(K)$ 13

1.2.4 The Infinite Descent: Computing $E(K)$ from $E(K)/2E(K)$ 14

1.3 Applications of Computing the Mordell-Weil Group 15

1.3.1 Describing Rational Solutions to Elliptic Diophantine Equations. 15

1.3.2 Integral Points on Elliptic Diophantine Equations. 16

1.3.3 Rational Points on Certain Curves of Genus > 1. 17

1.3.4 Rational Points on Certain Surfaces. 18

1.4 Computer Packages 19

1.4.1 `mwrank` and `findinf` 19

1.4.2 `Pari/GP` 19

2 The Infinite Descent **21**

2.1 The bound on the difference $h(P) - \hat{h}(P)$ 21

2.1.1 Preliminaries 21

2.1.2 υ is Real . . . 30
2.1.3 υ is Complex . . . 31
2.1.4 υ is Non-Archimedean . . . 33
2.1.5 The Height Modulo Torsion . . . 34
2.1.6 Examples . . . 35
2.2 The Canonical Height and Results from the Geometry of Numbers 38
2.3 A Sub-lattice Enlargement Procedure . . . 42
2.3.1 Sieving . . . 43
2.3.2 Solving the Equation $P = pQ$ . . . 44
2.4 Examples . . . 46

3 Computing the 2-Selmer Group of an Elliptic Curve **54**
3.1 The Method of Brumer and Kramer . . . 55
3.2 Finding $K(R, 2)$ . . . 57
3.3 Computing The 2-Selmer Group . . . 60

4 Descents on the Intersections of 2 Quadrics **63**
4.1 Introduction . . . 63
4.2 The Homogeneous Spaces for the 2-Descent . . . 65
4.3 'Coprimality' in number fields . . . 66
4.4 Diagonalization . . . 68
4.5 Parametrization of the Singular Combinations . . . 69
4.6 Descents . . . 71
4.6.1 F has at least 2 roots defined over K . . . 71
4.6.2 F is the Product of 2 Irreducible Quadratic Factors . . . 73
4.6.3 F has exactly one root defined over K . . . 75
4.7 Examples . . . 79
4.8 Local to Global- A Counter Example . . . 81

5 Local Solubility I: Over Non-Archimedean Completions **86**
5.1 Introduction . . . 86
5.2 Algorithm I . . . 87

5.3 Algorithm II: F has a rational root over $\mathcal{O}_v$ 90
5.3.1 Parametrizing the Singular Combination 90
5.3.2 Local Solubility Testing for $Y^2 = g(X)$ 91

6 Local Solubility II: Over Archimedean Completions 96
6.1 Introduction 96
6.2 Reducing to Totally Real $F(\lambda)$ 97
6.3 Results on the Totally Real Case 98
6.4 The Algorithm 100
6.5 A Special Case for Two Quadrics in Four Variables 100

A Hensel Lifting for $Y^2 = g(X)$ 102

B The Geometry of the Intersection of two Quadrics 104
B.0.1 The Combinant 107