

Much of the information in these notes is the result of machine computation; however the theoretical basis of these computations is not always trivial. *Birch and Swinnerton-Dyer* [2]

1 Introduction: The Age of Experimental Mathematics

Astronomers and biologists have had telescopes and microscopes respectively to aid in their research. With the advent of the computer, mathematicians acquired a powerful tool, using which they could generate data, make conjectures and try turning them into theorems — this was the dawn of the golden age of experimental mathematics.

My research sits at the crossroads of number theory, algorithms and computation. The problems and conjectures which pique my interest are the ones which have the potential of giving us an insight into the computational complexity of problems and the underlying mathematics. A fondness for the building blocks of modern number-theoretic cryptography — integer factoring and computing discrete logarithms — also influence the problems I choose to investigate. For instance, my excursion into number theory had a cryptographic motivation, namely trying to understand the Semaev-Smart-Satoh-Araki attack on the elliptic curve discrete logarithm problem [22]. This naturally lead to the question of deciding whether the p -part of a certain group is nontrivial — see §3.2. Proceeding from the above to computing elliptic curve rational torsion and in turn to the BSD conjecture has been a wonderful introduction to a world where conjectures abound and computations are indispensable. This document captures past and current work and outlines my plans for future research.

My thesis revolves around the BSD (Birch and Swinnerton-Dyer) conjecture for elliptic curves defined over the rational numbers, a famous problem that has been open for over forty years and one of the seven Millennium Prize problems [20]. This conjecture is considered to be the first nontrivial number theoretic problem put forth as a result of explicit machine computation — in the late '50s at Cambridge University. The BSD conjecture relates the *rank* of the Mordell-Weil group, the group of rational points of an elliptic curve, a quantity which seems to be difficult to pin down, to the order of vanishing of the L-series of the elliptic curve at its central point. The problems I investigate in my thesis are motivated by viewing this conjecture and its formula — which is a bridge which connects algebraic objects to complex analytic ones — from a computational perspective.

In what follows, I will share with the reader a glimpse of the contents of my thesis on a chapter-by-chapter basis — §2–§5, §8 — and proceed to enumerate questions which arise and problems I plan to work on including ones not related to my thesis. Section 2 states the conjecture of Birch and Swinnerton-Dyer and sets up notation and definitions for the rest of this document. Section 3 presents an efficient randomized algorithm for elliptic curve rational torsion computation. Section 4 concerns a family of certain quartic twists of the elliptic curve $y^2 = x^3 - x$, which raises interesting questions about integer factoring and heights of rational points. The latter we address in §5 by comparing the situation to the multiplicative group scenario and the Brauer-Siegel theorem. Next, in §6, projects involving Heegner point machinery are discussed. Section 7 states initial work involving modular Galois representations and the *method of graphs* algorithm. My involvement with the SAGE project is sketched in §8. Finally, §9 elaborates on my career plans.

Note. Elliptic curves will be defined over \mathbb{Q} ; p, q and l will denote primes numbers, unless stated otherwise. In time complexity analysis we present, a time step is a bit operation. \tilde{O} notation is defined to be the terms appearing in the Big-Oh notation modulo factors sublinear in the length of input. Everything is joint work with Ming-Deh Huang, unless stated otherwise.

2 Birch and Swinnerton-Dyer Conjecture

An *elliptic curve* defined over a field K is a smooth curve of genus 1 over K together with a K -rational point. Such a curve is given by a nonsingular affine curve $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, where $a_i \in K$.

Let E be an elliptic curve defined over \mathbb{Q} . A theorem of Mordell states that $E(\mathbb{Q})$ is a finitely generated abelian group. Hence $E(\mathbb{Q}) = E(\mathbb{Q})_{tors} \times \mathbb{Z}^r$, where $E(\mathbb{Q})_{tors}$ is the torsion subgroup, finite in size and r is the arithmetic rank of $E(\mathbb{Q})$. Let r_E^{an} and r_E denote the analytic and arithmetic rank of E which are the order of

vanishing of L -function of E $L_E(s)$ at $s = 1$ and the abelian group rank of $E(\mathbb{Q})$ respectively. The fascinating conjecture is as follows:

Conjecture 2.1 (*Birch and Swinnerton-Dyer*)

$$r_E^{an} = r_E \quad (1)$$

$$\frac{L_E^{(r_E)}(1)}{r_E!} = \#\text{III}(E) \cdot R(E) \cdot \Omega \cdot \prod_p c_p \cdot (\#E(\mathbb{Q})_{tors})^{-2} \quad (2)$$

The left hand side of Eq.(2) denotes the leading coefficient of the Taylor expansion of $L_E(s)$ at $s = 1$. The terms on the right hand side of the formula are: $\#\text{III}(E)$ is the size of $\text{III}(E)$, the Shafarevich-Tate group of E (see §6.2), Ω is defined to be $\int_{E(\mathbb{R})} |\omega|$, where $\omega := dx/(2y + a_1x + a_3)$ is the invariant differential on a global minimal Weierstrass equation for E over \mathbb{Q} ; $R(E)$ stands for the elliptic regulator of $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$, computed using the canonical height pairing; and $c_p := \#E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ refers to the Tamagawa number at p , where $E_0(\mathbb{Q}_p)$ is the subgroup of the group of \mathbb{Q}_p -points of E that reduce to a non-singular point on the reduced curve at p . Two reasons which make this conjecture interesting are: $\text{III}(E)$ is known to be finite only in a few cases and only in the last decade or so was it shown that the left hand side of formula is well-defined [3].

3 Computing elliptic curve torsion

This section sketches our efficient algorithm to compute one of the invariants appearing in Eq.(2).

3.1 Elliptic curve rational torsion

Let E/\mathbb{Q} be an elliptic curve defined by $y^2 = x^3 + ax + b$, where $a, b \in \mathbb{Z}$ and its discriminant $\Delta := -16(4a^3 + 27b^2)$. Any elliptic curve over \mathbb{Q} can be efficiently transformed to the above form. I would like to thank Noam Elkies for pointing out that the running times of the algorithms [5] being polynomials in $\log |\Delta|$ are conditional on the weak version of Szpiro's conjecture.

Theorem 3.1 *There is a randomized algorithm which computes $E(\mathbb{Q})_{tors}$ in $\tilde{O}(\log H(E))$ expected time. The deterministic version of the algorithm runs in $\tilde{O}(\log^2 H(E))$ time, where $H(E) = \max\{|a^3|, |b^2|\}$.*

A theorem of Nagell-Lutz states that a nontrivial torsion point of E , has integral coordinates and either its y -coordinate is 0 or divides $4a^3 + 27b^2$. The latter implies that the magnitude of the coordinates of torsion points are $O(|\Delta|)$. A naive procedure using the theorem to compute torsion would be computationally expensive. Our algorithm computes these integral points l -adically upto $O(\log_l |\Delta|)$ l -adic precision using division polynomials, Mazur's $E(\mathbb{Q})_{tors}$ classification theorem and Hensel lifting. The prime l is chosen such that $l > 7, l \nmid \Delta$ and l is small compared to $|\Delta|$.

In practice computing $E(\mathbb{Q})_{tors}$ gives rise to the following question: 'what is a bound for when the sequence $\{\gcd(\{\#E(\mathbb{F}_l) \mid l \text{ is a odd prime of good reduction}\}_{l \leq X})\}_X$ stabilizes?'. This question becomes more interesting in the elliptic curve over number field setting — see §3.3.

Project 3.1 *In joint work with Charles Denis, I am working on the above question based on an idea of Felipe Voloch. The answer would also give some information about the existence of isogenous curves in some cases [15].*

3.2 Deciding whether $E(\mathbb{Q}_p)[p] \neq 1$

Due to the existence of the Weil pairing, for $p > 2$, $\#E(\mathbb{Q}_p)[p]$ is either trivial or has size p — the size being p^2 is ruled out. In [4, 5], we devised an algorithm — polynomial in $\log p$ and $\log H(E)$ — that decides whether an E/\mathbb{Q} has a nontrivial p -torsion part. The algorithm has two subroutines, one of which handles the case of E having split multiplicative reduction at p . If $\#E(\mathbb{Q}_p)[p] = 1$ then the triviality of $E(\mathbb{Q})[p]$ is implied and therefore this procedure could be useful to compute $E(\mathbb{Q})_{tors}$ in practice.

3.3 Computing Elliptic curve number field torsion

To extend these ideas to an elliptic curve over a number field K , though results à la Mazur are not known for large degree extension fields we can instead obtain an upper bound for the group size by computing the size of group of the elliptic curve over the residue field for a few primes and determining their gcd. This endeavor of computing $E(K)_{tors}$ will require working efficiently with extensions of \mathbb{Q} and \mathbb{Q}_p , their associated rings of integers and residue fields. A nontrivial computation is to reconstruct the root of an m -division polynomial from its \mathfrak{p} -adic approximation, where \mathfrak{p} is a prime ideal of K [1].

Project 3.2 *Analyze the time complexity and implement the algorithm efficiently in SAGE [26].*

4 Notes on certain quartic twists of an elliptic curve

In [6, 7] we investigate elliptic curves of the form $E = E_D : y^2 = x^3 - Dx$, where $D = pq$ with p and q distinct prime numbers, $p \equiv q \equiv 3 \pmod{16}$. These are quartic twists of $y^2 = x^3 - x$. Employing the method of two-descent, we show that under BSD, the Mordell-Weil rank of E is one. Specifically,

Lemma 4.1 *Let E be as above. Assuming $r_E^{an} = 1$ (or alternatively the BSD conjecture), $r_E = 1$.*

Suppose $E(\mathbb{Q}) = \langle T \rangle + \mathbb{Z}P$, where $T = (0, 0)$, we prove that the valuations of $x(P)$ with respect to p and q are different $v_p(x(P)) \neq v_q(x(P))$. The above is shown using the fact that if R is a rational point on E , $R \neq O, T$ then using the group law formulae we arrive at the identity $x(R) \cdot x(R + T) = -pq$. This sets the stage for the reduction between the problem of factoring integers D and the problem of computing rational points on E_D . The complexity of the reduction raises the following question: *How is the minimal height of a rational non-torsion point of E_D upper-bounded by $\Delta(E_D)$? — see §5.*

Project 4.1 *Speed up computation of $L'(E_D, 1)$ by calculating the traces of Frobenius using the quartic residue symbol and compute $R(E_D) \cdot \#\text{III}(E_D)$ for a large number of curves.*

If $L'(E_D, 1) \neq 0$ then the rank of $E_D(\mathbb{Q})$ is equal to 1 by the work of Kolyvagin [16]. Unconditionally proving that a positive density of these have $r_{E_D} = 1$ will be an interesting exercise to acquire analytic skills. Thanks to Kannan Soundararajan for the quadratic twist case [19] reference.

5 Brauer-Siegel Analogue

I would like to thank Joseph Silverman for helpful discussions related to this section. The height of a rational point on an elliptic curve measures the *size* of the point. We turn to the literature — Lang’s conjectures — to obtain bounds on the heights of generators of $E(\mathbb{Q})$ and understand this phenomenon better.

Conjecture 5.1 [18] *Let $H(E) = \max(|a|^3, |b|^2)$. For all elliptic curves $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}$, we have $\#\text{III}(E) \cdot R(E) \ll H(E)^{1/12} N^{\epsilon(N)} c^{r_E} (\log N)^{r_E}$ with N is the conductor of the curve, c is some universal constant, and $\epsilon(N) \rightarrow 0$ as $N \rightarrow \infty$. In fact, $\epsilon(N)$ may have the explicit form $\epsilon(N) = c'(\log N \log \log N)^{-1/2}$.*

The enormous gap between the lower bound — conjecturally $O(\log |\Delta|)$ [18] — and the above upper bound, prompted the comparison of this scenario with that of the multiplicative group, the Brauer-Siegel theorem [9], which leads to the following question: if $\{E_i\}$ is a family of elliptic curves defined over \mathbb{Q} satisfying the condition: $\lim_{i \rightarrow \infty} |\Delta(E_i)| = \infty$, then $\lim_{i \rightarrow \infty} \frac{\log(\#\text{III}(E_i) \cdot R(E_i))}{\log |\Delta(E_i)|} = \frac{1}{12}$?

Project 5.1 *To understand this question better, we are currently doing computations [7] with the aforementioned family of quartic twists (§4) and elliptic curve databases [11, 25]. Observe that if we consider bounded regulators then we obtain information on the size of the Shafarevich-Tate group, subject to the above conjecture.*

6 Heegner points and applications

In this section we highlight projects about Heegner points, which can be used to construct not just rational points but also elements of the Shafarevich-Tate group of an elliptic curve.

6.1 Computing $E(\mathbb{Q})$

A part of my introduction to this topic was at the Arizona Winter School 2006 [21], where the team I was part of a team — mentored by Henri Cohen — which implemented the Heegner point method [12] in Pari-Gp. Suppose E/\mathbb{Q} with conductor N and analytic rank $r^{an} = 1$ then this procedure computes a rational point on an elliptic curve using complex analytic techniques, namely leveraging the structure of the modular curve $X_0(N)$.

Let d be the discriminant of a imaginary quadratic field K wherein the primes dividing N split such that the quadratic twist of E by d has rank 0. The Heegner point method constructs a point y_K in $E(K)$ — which turns out to be an elliptic curve rational point — using the modular parameterization $\varphi : X_0(N) \rightarrow E$ and the Gross-Zagier formula. Heegner point method is computationally expensive for elliptic curves of large conductor, but this is reasonable assuming that the height of elliptic curve rational points get “big”. This leads to the open question of considering an elliptic curve E such that $r^{an} = 1$ with a generator having “small” height and asking whether the arithmetic of $X_0(N)$ can be used to find a rational point in time polynomial or subexponential in the height.

This method turning into a reasonable algorithm is contingent on the fact that there exists a suitable discriminant d and the time complexity of finding one such discriminant. The former holds due to the work of Bump and others who proved that there are infinitely many such d . The latter remains unclear, though in practice such a discriminant is found in a few tries.

Project 6.1 *Given an E/\mathbb{Q} with $r_E^{an} = 1$, what is a bound on the number of discriminants that have to be tried before one is found which enables for a non-torsion rational point to be found using the Heegner point method? Perform explicit computation to estimate on this bound for curves in §4.*

6.2 Computing III

The Shafarevich-Tate group of E/\mathbb{Q} is defined as $\text{III}(E) = \ker(H^1(\mathbb{Q}, E) \rightarrow \bigoplus H^1(\mathbb{Q}_p, E))$, and this group measures the failure of the Hasse local-to-global principle, which states that an equation is solvable in \mathbb{Q} if and only if it is solvable in \mathbb{R} and \mathbb{Q}_p for each prime p . It is the nontriviality of this group which renders “local” methods unusable to finding rational points.

Kolyvagin [16] defined classes $c(n) \in H^1(K, E[p])$, from Heegner points of “conductor n ” for K , where K is as described in the previous subsection and n, p satisfy certain technical conditions. Let $d(n)$ be the image in $H^1(K, E)[p]$ of $c(n)$. He discovered criteria for the local triviality of the classes $d(n)$ in terms of local properties of the above Heegner points and used them to prove the BSD conjecture in the rank 1 case.

An approach to constructing elements of $\text{III}(E)$ is to compute $c(n) \in H^1(K, E)[p]$ and show that they are in fact nontrivial elements of $\text{III}(E)[p]$. Such an initiative has been undertaken by Dimitar Jetchev, Kristin Lauter and William Stein [23]. In [13] the authors present an algorithm which decides whether a Kolyvagin class $d(n)$ is a nontrivial element of $\text{III}(E/K)$ by (Cassels) pairing it with a certain *test class* $d(n')$. A natural and nontrivial question which the authors raise is the time complexity of producing such a test class.

Project 6.2 *In joint work with William Stein, I plan to obtain information about the order of $\#\text{III}(E)$ using p -adic (BSD) techniques and compute $\text{III}(E)$ using the above methods [23].*

7 Modular forms, Galois representations and Elliptic curves

Modular forms, Galois representations and elliptic curves (more generally abelian varieties), informally speaking are three sides of the same story, due to progress made in turning the Shimura-Taniyama conjecture (Modularity

theorem) [3] and Serre's conjectures [17] into theorems. I am interested in problems which have the following flavor: given either of the first two objects in a suitable description does there exist an elliptic curve over \mathbb{Q} which corresponds to them and if so construct the latter. Two projects in this vein are summarized in the following two subsections.

7.1 Modular Galois representations

Let E/\mathbb{Q} be an elliptic curve and $E[p]$ the p -torsion group of E . The latter is a Galois module using which one can construct a continuous Galois representation: $\bar{\rho} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{F}_p)$. Conversely, Serre conjectured that such an irreducible odd $\bar{\rho}$ is modular, that is, *arises from* a newform $f \in S_k(\Gamma_1(N))$ of prescribed weight $k = k(\bar{\rho})$ and level $N = N(\bar{\rho})$. In very recent work [17] Chandrashekhara Khare and collaborators have proved that for $p > 2$, Serre's conjecture is true for odd conductors.

Project 7.1 *It is known that $\bar{\rho}$ need not arise from an elliptic curve, unless $p = 2, 3, 5$ [10]. Working with Luis Dieulefait, I am investigating the $p = 7$ scenario using theory and computation.*

7.2 Method of graphs

The method of graphs developed by J.-F. Mestre and J. Oesterlé allows one to obtain a basis for $S_2(\Gamma_0(N))$, the space of cusp forms of weight k and level N , when N is prime. At a workshop at MSRI [24], in joint work with David Kohel and William Stein, we implemented code which is part of SAGE, which computes the action of Hecke operators on the above space. We do not explicitly compute the modular forms and corresponding elliptic curves and the bulk of the computation — computing kernel of the l^{th} Hecke operator T_l on $S_2(\Gamma_0(pM))$ for the first few primes l — is linear algebra. The latter is nontrivial as the dimension of the space involved grows linearly in the level pM . The elliptic curve $y^2 + xy = x^3 - x^2 - 79x + 289$ with conductor $234446 = 2 \cdot 117223$ is rank 4. Another goal of the project [23], is to check if any rank 4 curve with smaller (composite) conductor exists by comparing the data generated by the method of graphs procedure to the curves in [25].

Project 7.2 *Use the method of graphs to find all elliptic curves of conductor $N \leq 234446$, for all integers N that are either prime or of the form pM with p prime and $M \leq 10$ or $M = 12, 13, 16, 18$.*

8 SAGE

SAGE - Software for Algebra and Geometry Experimentation [26] is a free, *open source* software system for research in algebra, geometry, number theory and allied areas. I use SAGE and its components — Pari, mwrank, etc. — for all my computation. I have been actively involved in the SAGE community since its early days, scripting, providing feedback on design, posting bugs, giving talks. (Also see my teaching statement for the undergraduate research initiative involving SAGE.) I am one of the organizers of a conference titled *Workshop: Interactive Parallel Computation in Support of Algebra, Geometry and Number Theory* [8], which will take place in January 2007 at MSRI, Berkeley. Some of the goals of this workshop are to incorporate practical parallel algorithms into SAGE, and to make possible distributed computation of large tables of elliptic curves and modular forms. I will be writing a chapter of my thesis on the topic of SAGE and parallelism.

9 Career Plans

The position I am applying for is a stepping stone toward a tenured member of the faculties of the Computer Science and Mathematics departments. In the interim period, I plan to establish myself as a researcher working on understanding fundamental problems in number theory and cryptography such as: the finiteness of the Shafarevich-Tate group, the BSD conjecture [16], and the hardness of discrete logarithm problems [14]. I expect the theme of my research career to be shaped by the interesting arithmetic phenomena and questions which will emerge as the limits of practical computation get pushed further.

References

- [1] Belabas, K. *A relative van Hoeij algorithm over number fields*. J. Symbolic Computation, Vol 37 (2004), no. 5, pp. 641-668.
- [2] Birch, B. J., Swinnerton-Dyer, H. P. F. *Notes on elliptic curves. I*. J. Reine Angew. Math. 212 1963 7–25.
- [3] Breuil, C., Conrad, B., Diamond, F., and Taylor, R., *On the modularity of elliptic curves over \mathbb{Q} : wild 3-adic exercises*, J. Amer. Math. Soc. 14 (2001), no. 4, 843-939 (electronic).
- [4] Burhanuddin, I.A., Huang, M.-D. *Deciding whether the p -torsion group of the \mathbb{Q}_p -rational points of an elliptic curve is non-trivial*. ANTS VI Poster Abstracts, SIGSAM Bulletin, Volume 38, Number 3, September 2004, Issue 149, 96–98.
- [5] Burhanuddin, I.A., Huang, M.-D. *Elliptic curve torsion points and division polynomials*. Computational aspects of algebraic curves, T. Shaska (ed.), Lecture Notes Series on Computing, 13 (2005), 13–37, World Scientific.
- [6] Burhanuddin, I.A., Huang, M.-D. *Factoring integers and computing elliptic curve rational points*. USC Computer Science Technical Report 06-875.
- [7] Burhanuddin, I.A., Huang, M.-D. *Notes on certain quartic twists of an elliptic curve*. In preparation.
- [8] Burhanuddin, I.A.; Demmel, J.; Goins, E.; Kaltofen, E.; Perez, F.; Stein, W.; Verrill, H.; Weening, J. *Workshop: Interactive Parallel Computation in Support of Algebra, Geometry and Number Theory*. <http://modular.math.washington.edu/msri07>
- [9] Brauer, R. *On zeta-functions of algebraic number fields*, Amer. J. Math. 69, Num. 2, 1947, pp.243-250.
- [10] Calegari, F. *Mod p representations on Elliptic Curves*. <http://www.math.northwestern.edu/~fcale/>
- [11] Cremona, J.E. *Elliptic Curve Data*. <http://www.maths.nott.ac.uk/personal/jec/ftp/data>.
- [12] Cohen, H. *Number Theory. Part II: Analytic and Modern Methods*. In press.
- [13] Eisenträger, K., Jetchev, D., Lauter, K. *On the Computation of the Cassels Pairing for certain Kolyvagin classes in the Shafarevich-tate group*. <http://research.microsoft.com/~klauter/>
- [14] Huang, M.-D., Raskind, W. *Global Methods for Discrete Logarithm Problems, I, II and III*, 2006. <http://www-rcf.usc.edu/~mdhuang/papers.html/>.
- [15] Katz, N. M. *Galois properties of torsion points on abelian varieties*. Invent. Math. 62 (1981), no. 3, 481–502.
- [16] Kolyvagin, V. A. *Euler Systems*, In The Grothendieck Festschrift, Vol. 2 (Ed. P. Cartier et al.). Boston, MA: Birkhäuser, pp. 435-483, 1990.
- [17] Khare, C. *Modularity of Galois representations and motives with good reduction properties*. <http://www.math.utah.edu/~shekhar/papers.html>
- [18] Lang, S. *Conjectured Diophantine estimates on elliptic curves*. Arithmetic and geometry, Vol. I, Progr. Math., vol. 35 (1983), 155–171.
- [19] Perelli, A., Pomykala, J., *Averages of twisted L-functions*, Acta Arithmetica, (1997), 149 -163.
- [20] *Millennium Prize Problems*. <http://www.claymath.org/millennium/>.
- [21] Rodriguez-Villegas, F. et al. *Arizona Winter School: Computational and algorithmic aspects of algebra and arithmetic*. <http://math.arizona.edu/~swc/oldaws/06GenlInfo.html>
- [22] Semaev, I. *Evaluation of discrete logarithms in a group of p -torsion points of an elliptic curve in characteristic p* . Mathematics of Computation, 67:353–356, 1998.
- [23] Stein, W. *NSF Proposal: Explicit Approaches to the Birch and Swinnerton-Dyer Conjecture* <http://sage.math.washington.edu/grants/stein-antc-06/>.
- [24] Stein, W. *Workshop: Computing with Modular Forms*. <http://sage.math.washington.edu/msri06>.
- [25] Stein, W., Watkins, M. *Elliptic Curve Database*. <http://sage.math.washington.edu/papers/stein-watkins/>.
- [26] Stein, W., Joyner, D. *Sage: System for algebra and geometry experimentation*, Communications in Computer Algebra (SIGSAM Bulletin) 39 (June 2005), no. 2. <http://sage.math.washington.edu/sage>.