

Research Statement

Stefan Erickson

My background and main interest is in algebraic number theory. My thesis problem was to extend the First Order Stark Conjecture to cases previously not considered. Roughly speaking, the Stark Conjectures form a link between the derivatives of L -functions at $s = 0$ for Galois extensions K/k and certain algebraic units in K . I was able to show that under certain conditions that the extended conjecture follows from the original conjectures for the intermediate extensions.

Recently, my research interests have shifted towards elliptic and hyperelliptic curve cryptography. I am fascinated by the idea of using algebraic curves to encode information. It applies many theoretic tools of arithmetic geometry and complex multiplication. Elliptic curve cryptography currently provides the fastest known methods for a given security level.

I also feel that there is much more potential for getting undergraduate students involved in cryptography. There are still many open problems which can be easily understood and implemented by students with a basic background in number theory and abstract algebra. Last summer, an undergraduate student of mine and I received a Colorado College Venture Grant to fund our summer research project to develop explicit formulas for cryptography. I plan to support undergraduate research for a long time to come.

Elliptic and Hyperelliptic Curve Cryptography

Elliptic curves can be expressed as

$$y^2 = x^3 + ax + b$$

for some coefficients a and b . It is possible to define an “addition” law, which turns the points of an elliptic curve into an abelian group. Elliptic curves can be used for cryptographic protocols by taking the coefficients and coordinates in a finite field of large prime order.

Given a point P and an integer n , it is relatively easy to compute nP . On the other hand, given points P and $Q = nP$, it is very hard to recover n . The difficulty of this “discrete logarithm problem” is the basis of the Diffie-Hellman Key Exchange protocol. In contrast with modular arithmetic, there is no known subexponential algorithm for solving the discrete logarithm problem for elliptic curves, which allows for using much smaller fields and hence faster speeds in cryptographic systems. This has important applications when there are limits in processor speed or bandwidth, such as cell phones or personal handheld devices.

Hyperelliptic curves are similar to elliptic curves, but replaces the cubic with a higher degree polynomial $f(x)$. Although there is no natural group law on points of hyperelliptic curves as with elliptic curves, one can use the Jacobian of hyperelliptic curves over finite fields for cryptographic protocols.

I am interested in several problems related to elliptic and hyperelliptic curves.

- (Explicit Arithmetic Formulas) For a generic curve of a certain type over a finite field, find explicit formulas for addition and doubling with as few field operations as possible.
- (Pairing-Friendly Curves) Construct special curves which are conducive to pairing-based applications.

Hyperelliptic curves come in two kinds, imaginary (when the degree of f is odd) and real (when the degree of f is even). A recent paper of Jacobson, Scheidler, and Stein has made significant improvements on algorithms for implementing cryptosystems based on the infrastructure of real hyperelliptic curves. [JSS07] In their initial tests, the real curves have been shown to be competitive with imaginary curves. These tests were based on a general implementation of Cantor’s algorithm. In reality, there are explicit formulas which have been optimized in the imaginary cases. [La05]

In [EJSS07], we provided for the first time explicit formulas for divisor arithmetic on genus 2 real hyperelliptic curves in affine coordinates, with an improvement of two to three times faster than generic methods. We also found an improvement on the explicit formulas for imaginary genus 2 curves. Arithmetic on real curves is now almost as fast as imaginary curves. This result has important consequences for curve construction problems, since most curves generated by CM methods are real curves. We will soon provide more general formulas which will appear in a future journal article. I am currently developing formulas in projective coordinates with an undergraduate student of mine, Tra Ho.

A recent development in elliptic curve cryptography is using bilinear maps (called pairings) from elliptic curves into the roots of unity of an extension of the base field. There are several important applications of pairings, including key exchange between three parties and identity-based encryption. There are only a handful of families of elliptic curves (MNT curves and its variants) which are suitable for implementing these pairings. The only known family of pairing-friendly hyperelliptic curves have finite fields too large for practical use in cryptography. [Fr07] I am currently working on producing families of pairing-friendly genus 2 hyperelliptic curves with Kristin Lauter at Microsoft Research and Ning Shang at Purdue University.

The Stark Conjectures

Hilbert's Twelfth Problem asks for a method of constructing abelian extensions of number fields using analytic functions. Although class field theory provides a classification of the maximal abelian extensions of global fields, the explicit construction is only known in a few cases. The Kronecker-Weber Theorem states that every abelian extension of the rationals is contained in a cyclotomic extension, which can be generated via the exponential function. The theory of complex multiplication uses elliptic functions to produce the maximal abelian extensions of complex quadratic fields. The torsion points of rank 1 Drinfeld modules are used in the case of function fields.

In the 1970's, Harold Stark [St] conjectured the existence of certain algebraic units which evaluate the first derivatives of abelian L -functions at $s = 0$. John Tate [Ta] showed that under certain circumstances, these units would lead to an explicit generation of maximal abelian extensions of the base field. Since the L -functions can be approximated on computers, one can effectively compute the unit and its conjugates to many decimal places and thus find the polynomial it satisfies. Hence, Stark conjecturally provides an answer to Hilbert's Twelfth Problem in many situations.

The setting of the Stark Conjectures is imprimitive L_S -functions, where S is a finite set of primes in the base field k including all ramified and infinite primes. Let K/k be a finite abelian extension of number fields with Galois group G and group of characters \hat{G} . For $\text{Re}(s) > 1$, the imprimitive L -function of χ and S is given by

$$L_S(s, \chi) = \prod_{\mathfrak{p} \notin S} \left(1 - \frac{\chi(\sigma_{\mathfrak{p}})}{\mathbf{N}\mathfrak{p}^s} \right)^{-1}$$

where \mathfrak{p} ranges over all finite unramified primes not in S and $\sigma_{\mathfrak{p}}$ is the Frobenius automorphism associated to \mathfrak{p} .

If all the L_S -functions vanish at $s = 0$ with at least a first order zero (that is, $L_S(0, \chi) = 0$ for all $\chi \in G$), then the First Order Stark Conjecture states that there is an S -unit ε which evaluates the first derivatives:

$$L'_S(0, \chi) = -\frac{1}{w_K} \sum_{\sigma \in G} \chi(\sigma) \log |\varepsilon^\sigma|_{\mathfrak{p}_0}$$

for all $\chi \in \hat{G}$, where w_K is the number of roots in K . Furthermore, $K(\varepsilon^{1/w_K})/k$ should be an abelian extension.

Originally, the First Order Stark Conjecture was only formulated when S contained a prime which split completely. This condition is sufficient to force all the L_S -functions to have a first order zero. However, there are many sets S which contain no splitting prime, but $L_S(0, \chi) = 0$ for all χ . My thesis problem was to extend the conjectures to these "1-covers."

In [Er08], I developed a theoretical framework for the Extended First Order Stark Conjecture. I also showed that the extended conjecture follows from the original conjectures under certain conditions.

Theorem 1. *If S contains a 1-subcovering consisting of only unramified primes and at most one infinite prime, then the First Order Stark Conjecture implies the Extended First Order Stark Conjecture.*

Theorem 2. *If K/k is a multiquadratic extension of degree 2^m and $\#S > m + 1 - r$ where r is the 2-rank of the S_{fin} -class group of k , then Extended First Order Stark Conjecture is true.*

I have also numerically verified the extended conjecture over totally real cubic and quintic fields. I hope to continue to work in this direction.

References

- [Er05] S. Erickson, *New settings of the first order Stark conjecture*.
Ph.D. Dissertation, UC San Diego (2005).
- [Er08] S. Erickson, *An extension of the first order Stark conjecture*.
To appear in the Rocky Mountain Journal of Mathematics.
- [EJSS07] S. Erickson, M. J. Jacobson, Jr., N. Shang, S. Shen and A. Stein,
Explicit arithmetic formulas for real hyperelliptic curves of genus 2 in affine representation.
Arithmetic of Finite Fields, Lecture Notes in Computer Science **4547**, Springer, (2007).
- [Fr07] D. Freeman, *Constructing pairing-friendly genus 2 curves over prime fields with ordinary Jacobians*.
Pairing-Based Cryptography - Pairing 2007, Springer LNCS **4575**, (2007), 152-176.
- [JSS07] M. J. Jacobson, Jr., R. Scheidler and A. Stein, *Cryptographic protocols on real hyperelliptic curves*.
Advances in Mathematics of Communications **1** (2007), 197-221.
- [La05] T. Lange, *Formulae for Arithmetic on Genus 2 Hyperelliptic Curves*.
AAECC Journal **15**, (2005), 295-328.
- [St] H. M. Stark, *L-functions at $s = 1$, I, II, III, IV*,
Adv. in Math. **7** (1971), 301-343; **17** (1975), 60-92; **22** (1976), 64-84; **35** (1980), 197-235.
- [Ta] J. Tate, Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$,
Progr. in Math **47**, Birkhäuser Boston Inc, (1984).