The Function Field Sieve

Leonard M. Adleman

Department of Computer Science
University of Southern California
Los Angeles, California, 90089
Adleman@cs.usc.edu

Abstract. The fastest method known for factoring integers is the 'number field sieve'. An analogous method over function fields is developed, the 'function field sieve', and applied to calculating discrete logarithms over GF(p^n). An heuristic analysis shows that there exists a c ∈ ℝ₀ such that the function field sieve computes discrete logarithms within random time:

\[ L_{p^n}[1/3, c] \]

when \( \log(p) \leq n^{o(n)} \), where \( g \) is any function such that \( g : N \rightarrow \mathbb{R}_{\leq 0} \) approaches zero as \( n \rightarrow \infty \).

1 Introduction

It is well known that algebraic number fields and algebraic function fields with finite constant field - the so called global fields - share a rich theory. In this paper we generalize the 'number field sieve' [LL1, Adl, Co1, Go1, Go2] from algebraic number fields to algebraic function fields.

In the number field sieve a positive integer \( n \) is given. One finds an irreducible polynomial \( f \in \mathbb{Z}[y] \) of degree \( d \) and an \( m \in \mathbb{Z} \) such that \( f(m) = 0 \mod n \). Then working simultaneously in \( \mathbb{Q} \) and the number field \( L = \mathbb{Q}[y]/(f) \), one seeks 'double smooth pairs' \( < r, s > \in \mathbb{Z} \times \mathbb{Z} \) such that \( r \) and \( s \) are relatively prime and both \( rm + s \) and \( N_L^\mathbb{Q}(ry + s) = r^df(-s/r) \) are 'smooth' in \( \mathbb{Z} \) (i.e. have no prime factors greater than some predetermined 'smoothness bound' \( B \)). In the simplest case where \( O_L \), the ring of integers of \( L \), is a PID then from such a double smooth pair we have:

\[ rm + s = \prod_{i=1}^z p_i^{e_i} \]

where \( p_1, p_2, ..., p_z \) are the primes less than \( B \). And:

\[ ry + s = \prod_{i=1}^v \epsilon_i^{f_i} \prod_{i=1}^w p_i^{\beta_j} \]
where \( \epsilon_1, \epsilon_2, \ldots, \epsilon_v \) is a basis for the units of \( \mathcal{O}_L \) and \( \varphi_1, \varphi_2, \ldots, \varphi_w \in \mathcal{O}_L \) are generators of the (residue class degree one) prime ideals of norm less than \( B \).

Since there is a homomorphism \( \phi \) from \( \mathcal{O}_L \) to \( \mathbb{Z}/(n) \) induced by sending \( y \mapsto m \), the above equations give rise to the congruence:

\[
\prod_{i=1}^{v} p_i^{\epsilon_i} \equiv \prod_{i=1}^{u} \phi(\epsilon_i)^{\lambda_i} \prod_{j=1}^{w} \phi(\varphi_j)^{\delta_j} \mod n
\]

In the case that \( n \) is composite and its factorization is sought, one collects sufficiently many such double smooth pairs and puts the corresponding congruences together using linear algebra to create a congruence of squares of the form:

\[
(\prod_{i=1}^{v} p_i^{\epsilon_i})^2 \equiv (\prod_{i=1}^{u} \phi(\epsilon_i)^{\lambda_i} \prod_{j=1}^{w} \phi(\varphi_j)^{\delta_j})^2 \mod n
\]

Creating such congruences is tantamount to factoring \( n \).

In the case that \( n \) is prime and discrete logarithms in \( \mathbb{Z}/(n) \) are sought, one collects sufficiently many such double smooth pairs and uses linear algebra on the discrete logarithms of the corresponding congruences to solve for the discrete logarithms of the primes less than \( B \) [GoI].

Of course when \( \mathcal{O}_L \) is not a PID complications arise. These complications can be overcome by viewing the factorization of \( ry + s \) as an ideal factorization and introducing singular integers and character signatures [Adl]. At a conceptual level this approach makes the divisor associated with \( ry + s \) rather than \( ry + s \) itself central. The character signature of \( ry + s \) is introduced as a surrogate for the values of \( ry + s \) 'at infinity'.

In the 'function field sieve' one starts with a finite field \( F \) and a monic irreducible polynomial \( n \in F[x] \). One finds an absolutely irreducible polynomial \( H \in F[x, y] \) of degree \( d \) in \( y \) and an \( m \in F[x] \) such that \( H(x, m) \equiv 0 \mod n \). Then working simultaneously in \( F(x) \) and the function field \( L = \text{Quotient}(F[x, y]/(H)), \) one seeks 'double smooth pairs' \( < r, s > \in F[x] \times F[x] \) such that \( r \) and \( s \) are relatively prime and both \( rm + s \) and the intersection of \( ry + s \) with \( H, r^dH(x, -s/r) \) are 'smooth' in \( F[x] \) (i.e. have no irreducible factors of degree greater than the 'smoothness bound' \( B \)).

Having collected sufficiently many double smooth pairs, the approach taken now becomes value theoretic and geometric. The divisors of the \( ry+s \)'s are calculated. As usual there are difficulties 'at infinity'. The value of \( ry + s \) at the points at infinity on the smooth projective model of the affine curve associated with \( H \) are calculated geometrically using 'blow up'.