Relation Generation in Quadratic Number and Function Fields

Michael J. Jacobson, Jr.

jacobs@cpsc.ucalgary.ca

UNIVERSITY OF CALGARY

Joint work with J.-F. Biasse, A. Stein, and W. Trei

ANTD 2013

Imaginary Quadratic Number Fields

$\mathbb{Q}(\sqrt{\Delta}) = \{x + y\sqrt{\Delta} \mid x, y \in \mathbb{Q}\}$: quadratic field

- $\Delta \equiv 0, 1 \pmod 4$: discriminant ($\in \mathbb{Z}$, Δ or $\Delta/4$ square-free)
- $\Delta < 0$: *imaginary* quadratic field

$\mathcal{O}_\Delta \subset \mathbb{Q}(\sqrt{\Delta})$: maximal order of $\mathbb{Q}(\sqrt{\Delta})$ (ring of algebraic integers)

- $\mathcal{I}_\Delta$: group of invertible, fractional ideals of $\mathcal{O}_\Delta$
- $\mathcal{P}_\Delta$: principal, fractional ideals, subgroup of $\mathcal{I}_\Delta$
- $Cl_\Delta = \mathcal{I}_\Delta / \mathcal{P}_\Delta$: class group
- $h_\Delta = |Cl_\Delta|$: class number
- unique reduced ideal representatives of group elements

Relations

Relation: power-product of prime ideals that is principal

Used in index-calculus algorithms for:

- invariant computation (class number, class group structure, regulator/fundamental unit)
- discrete logarithm computation, principality testing / norm equations
- computing large-degree isogenies and endomorphism rings of ordinary elliptic curves over finite fields

Efficiency of all depends on quickly finding relations

Example: Computing the Class Group

Outline:

- factor base FB : prime ideals $\mathfrak{p}_i$ of norm $p_i \leq B$, must generate Cl_Δ
- surjective homomorphism (assume $|FB| = k$)

$$\varphi : \mathbb{Z}^k \to Cl_\Delta$$
$$(v_1, \dots, v_k) \mapsto [\mathfrak{p}_1^{v_1} \dots \mathfrak{p}_k^{v_k}]$$

- $\mathbb{Z}^k/\Lambda \cong Cl_\Delta$, where $\Lambda = \ker \varphi$ is the lattice of all relations wrt FB
- randomly construct generating system of Λ, linear algebra (Smith normal form) to compute group structure

Expected run time (GHR): $L_\Delta(1/2, \sqrt{2})$, where

$$L_\Delta(\alpha, \beta) = \exp((\beta + o(1))(\log|\Delta|)^\alpha(\log\log|\Delta|)^{1-\alpha})$$

Example: Computing Large-Degree Isogenies

$Ell_{t,u}(\mathbb{F}_q)$: isomorphism classes of elliptic curves over $\mathbb{F}_q$ with trace t and endomorphism ring $\mathcal{O}_{u^2\Delta_K} \in \mathbb{Q}(\sqrt{\Delta_K})$

Theorem

Let $\mathfrak{a} \subset \mathcal{O}_{u^2\Delta_K}$ be prime of norm ℓ. Then $\mathfrak{a}$ acts on $Ell_{t,u}(\mathbb{F}_q)$ via a degree ℓ isogeny, defining a faithful group action by $Cl_{u^2\Delta_K}$.

Jao, Soukharev 2010: idea (compute isogeny of degree ℓ):

- Compute relation $\mathfrak{p}_\ell \prod \mathfrak{p}_i^{e_i}$ in $Cl_{u^2\Delta_K}$ for p_i small, $N(\mathfrak{p}_\ell) = \ell$
- $[\mathfrak{p}_\ell] = \prod [\mathfrak{p}_i]^{-e_1} \in Cl_{u^2\Delta_K}$
- Evaluate the degree ℓ isogeny via evaluations of degree p_i isogenies

Expected run time (GRH): $L_q(1/2, \sqrt{3}/2) \log \ell$

Finding Relations

Main idea:

- Compute $\mathfrak{a} \sim \prod \mathfrak{p}_i^{e_i}$ (but not equal!)
- If $\mathfrak{a} = \prod \mathfrak{p}_i^{v_i}$, then $\prod \mathfrak{p}^{e_i - v_i}$ is principal

One approach: random selection of $\mathfrak{a}$ via choice of e_i (or random walks)

Better approach: sieving

- let $\alpha = ax + (b + \sqrt{\Delta})/2y \in \mathfrak{a} = a\mathbb{Z} + (b + \sqrt{\Delta})/2\mathbb{Z}$
- $N(\alpha) = a(ax^2 + bxy + cy^2)$ where $c = (b^2 - \Delta)/(4a)$
- there exists ideal $\mathfrak{b}$ with $N(\mathfrak{b}) = ax^2 + bxy + cy^2$ and $(\alpha) = \mathfrak{a}\mathfrak{b}$
- find $x, y \in \mathbb{Z}$ such that $f(x, y) = ax^2 + bxy + cy^2$ factors over the p_i

Sieving

Finding relations $\leftrightarrow$ finding smooth values of $f(X,Y) = aX^2 + bXY + cY^2$

One approach: find all $x \leq M$, $x \in \mathbb{Z}$, with $f(x,1) = ax^2 + bx + c$ smooth

For each prime ideal of norm p_i :

- compute root(s) r such that $f(r,1) \equiv 0 \pmod{p_i}$
- $p_i \mid r$, and $p \mid kp_i + r$ for all $k \in \mathbb{Z}$
- use analogue of Sieve of Eratosthenes to factor all $f(x,1)$ by "marking off" every p_ith cell in an array, starting at r

Can adapt quadratic sieve methods from integer factoring, including self-initialization

Some Results

Biasse (2010): class group for $\Delta = -4 \times 10^{110} - 4$

$$Cl_\Delta \cong \mathbb{Z}/857640364195029289112195513145214883828429420007144 0\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^{11}$$

Biasse, J. (2010): class group and regulator for $\Delta = 4 \times 10^{110} + 4$

$$Cl_\Delta \cong \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$R_\Delta \approx 70795074091059722608293227655184666748799878533480399.67302$$

4 days for relations (260 2.4 GHz Xeons), 4 days for linear algebra (2.4 GHz Opteron, 32 GB RAM), 4 days for GRH-verification

Isogeny and Endomorphism Ring Computation: Obstacles

Parameter tuning is really hard

- Composition of factor base can affect results dramatically
- Eg. (J. 1999), computing Cl_Δ
  - typical 70-decimal digit Δ : $18h$
  - 70-decimal digit Δ with no $p_i \leq 353$ in factor base: 6.5 days

Need really small factor bases for isogeny and endomorphism ring computation

- only small prime degree isogenies are efficient to compute
- sieving becomes more effective with larger factor bases

Our Approach (on-going work)

Analytic model to estimate smoothness probabilities given a particular factor base

- extend numerical methods to approximate $\psi(x, y)$ to ideals of quadratic fields
- would take into account differing splitting behavior of small primes
- use as basis of search for optimal parameters

Use Sutherland's improvements to evaluation of low-degree isogenies

- feasible to evaluate isogenies of larger prime degree
- may be sufficient to realize benefits from sieving

Imaginary Quadratic Function Fields

$C : y^2 + h(t)y = f(t)$ non-singular, $h, f \in \mathbb{F}_q[t]$

C is *imaginary* (genus g) if

- q is odd, $h = 0$, f monic and square-free with $\deg(f) = 2g + 1$
- q is even, $h \neq 0$ with $\deg(h) \leq g$ and f monic with $\deg(f) = 2g + 1$

(a.k.a. hyperelliptic curves)

$\deg 0$ divisor class group (ideal class group of $\mathbb{F}_q(C)$):

- finite abelian, size $\approx q^g$
- unique reduced divisor/ideal representatives of group elements

Example Application: Weil Descent

Reduce elliptic curve discrete logarithm problem (over $\mathbb{F}_{2^{ng}}$) to hyperelliptic curve discrete logarithm problem (genus g over $\mathbb{F}_{2^n}$)

- Enge, Gaudry (index-calculus): if $g > \log q$, expected run time $L_{q^g}(1/2, 5.73 + o(1))$
- J, Menezes, Stein: implementation, parameter optimization
  - solved ECDLP over $\mathbb{F}_{2^{31}}$, $\mathbb{F}_{2^{64}}$, $\mathbb{F}_{2^{93}}$, and $\mathbb{F}_{2^{124}}$
  - genus 31 hyperelliptic curves defined over $\mathbb{F}_2$, $\mathbb{F}_{2^2}$, $\mathbb{F}_{2^3}$, and $\mathbb{F}_{2^4}$
- Velichka, J., Stein: application of sieving, solved ECDLP over $\mathbb{F}_{2^{155}}$
  - genus 31 hyperelliptic curve defined over $\mathbb{F}_{2^5}$

Overview of Index Calculus and Sieving

Same general approach as in quadratic fields

- factor base: prime ideals $\mathfrak{p}$ with deg $p_i \leq B$ (p_i irreducible)
- find random relations
- solve linear algebra problem (linear system modulo group order)

Can apply same approach to finding relations, including sieving

- relation generation reduces to finding smooth values of $f(X) = aX^2 + bX + c$ defined over $\mathbb{F}_q[t]$
- same improvements (eg. self-initialization) are possible

Challenges with Sieving

Need to find all $x \in \mathbb{F}_q[t]$ with $\deg(x) \leq M$ such that $f(x)$ is B-smooth

How to map $x \in \mathbb{F}_q[t]$ to a cell in an array?

- Natural map (Flassenburg, Paulus 1998), $q = p^d$:

$$\nu : \mathbb{F}_q[t] \to \mathbb{Z}$$
$$x_m t^m + \cdots + x_0 \mapsto \nu_0(x_i) q^i + \cdots + \nu_0(x_0)$$

  where

$$\nu_0 : \mathbb{F}_q \to \{0, \ldots, q-1\}$$
$$\nu_0(a_d \alpha^d + \cdots + a_0) = a_d p^d + \cdots + a_0$$

Works, but painful to evaluate frequently

Challenges with Sieving, cont.

For irreducible $p_i \in \mathbb{F}_q[t]$ and $r \in \mathbb{F}_q[t]$ such that $f(r) \equiv 0 \pmod{p_i}$:

- how to rapidly find all $\nu(kp_i + r)$ for $k \in \mathbb{F}_q[t]$ such that $\deg(kp_i + r) \leq M$?
- map ν does not lead to regular spacing through the sieve array

Velichka, J., Stein 2008: enumerate all k of appropriate degree, evaluate $\nu(kp_i + r)$ directly using previous results and precomputations

- use $k'p_i + r = (kp_i + r) + (k' - k)p_i$ (add appropriate multiple of p)

Trei, J. Stein 2013: further optimizations, including

- evaluation at q using Horner's rule
- better use of intermediate results
- observation that $\nu(x + y) = \nu(x) \oplus \nu(y)$ (all ops on integers)

Numerical Results

VJS 2008 results (278 Intel P4 Xeon 2.4 GHz CPUs, 26 2.8 GHz):

- ECDLP over $\mathbb{F}_{2^{124}}$ (HCDLP with $g = 31$, $q = 2^4$):
  - 9 hours, 7.5 hours for relations (24 hours with random walks)
- First solution of ECDLP over $\mathbb{F}_{2^{155}}$ (HCDLP with $g = 31$, $q = 2^5$):
  - 3 weeks, 1 week for relations (random walks estimate 5 weeks)

TJS 2013 results (64 Intel Xeon X7560 2.27 GHz CPUs):

- $\mathbb{F}_{2^{124}}$: 3 hours (27 min. for relations)
- $\mathbb{F}_{2^{155}}$: in progress (2.5 days for relations)

Future Work

Complete analytic model to aid parameter selection

Two dimensional (lattice) sieving?

Batch smoothness test for candidates produced by the sieve?

Function fields:

- add double large primes
- try odd characteristic
- lower genus?