Factorization and DLP in a Subexponential Setting

Bogdan-Gabriel Ursu

University "Alexandru Ioan Cuza" of Iași
Faculty of Computer Science

bogdanbear@gmail.com
supervised by Prof. Dr. Ferucio Laurențiu Țiplea

June 28, 2015

Overview

Smooth integers

Definition

An integer a is said to be $y - smooth$ if $\forall p$ a prime integer with p/a, we have $p \leq y$.

L-notation

$L_n(\alpha, c) = e^{c \times log(n)^{\alpha} log(log(n))^{1-\alpha}}$, α is taken in $[0, 1]$.

- $\alpha = 0$, polynomial in the size of n, $L_n(0, c) = log^c(n)$.
- $\alpha = 1$, exponential complexity: $L_n(0, c) = n^c$.
- $\alpha \in (0, 1)$ sub-exponential complexity.

NFS

Number rings

Let $f \in \mathbb{Z}[x]$ irreducible with $f(m) \equiv 0 \ mod \ n$ (actually, $f(m) = n$) and $\alpha \in \mathbb{C}$ be one of the roots of f. The algebraic structure we collect relations from is the number ring $\mathbb{Z}[\alpha]$.

Factor-base

Consider small primes of degree 1 from $\mathbb{Z}[\alpha]$, associated with ring homomorphisms $\psi : \mathbb{Z}[\alpha] \to \mathbb{F}_q$ with $r_q = \psi(\alpha)$.

Compute a set S

$\prod_{(a,b)\in \mathbf{S}}(a - bm) = v^2$, with $v \in \mathbb{Z}$ and $\prod_{(a,b)\in \mathbf{S}}(a - b\alpha) = \gamma^2$, with $\gamma \in \mathbb{Z}[\alpha]$.

Factorize: $\phi(\gamma)^2 = v^2$, with $\phi : \mathbb{Q}[\alpha] \to \mathbb{Z}_{/n\mathbb{Z}}$, with $\phi(m) = n$.

Index Calculus in $\mathbb{Z}_{/p\mathbb{Z}}$

Discrete logarithm

Consider g a primitive root of $\mathbb{Z}_{/p\mathbb{Z}}$ and a random element $\beta \in \mathbb{Z}_{/p\mathbb{Z}}$, one needs to find the smallest power α such that $g^{\alpha} = \beta$.

Linear relations collection

Choose randomly $k \in \mathbb{Z}_{/(p-1)\mathbb{Z}}$, when lucky we have that $g^k = \prod_{s \in \mathbf{S}} s$, from which we obtain the linear relation: $k \equiv \sum_{s \in \mathbf{S}} log(s)$ mod n.

Compute individual logarithm

By randomly drawing k, express βg^k using only elements of the factor base: $\beta g^k = \prod_{s \in \mathbf{S}} s$. Taking logarithms of both sides as before, yields $k + \alpha = klog_g(\beta) = \sum_{s \in \mathbf{S}} log(s)\ mod\ n$ and therefore $\alpha = \sum_{s \in \mathbf{S}} log(s) - k\ mod\ n$.

Solving linear systems

Kernel approach

Used in QS, NFS and in Gaudry's algorithm for hyperelliptic curves. Less effort on linear relation collection but not useful for further computations. In the NFS, keep track of the order of each small prime from $\mathbb{Z}[\alpha]$ and then find a linear dependency.

Full rank approach Collect $|S| + \epsilon$ relations and obtain a full column rank matrix.

Problems

- logarithms of g belong to $\mathbb{Z}_{/(p-1)\mathbb{Z}}$, which is not a field. My solution: factorize $\mathbb{Z}_{/(p-1)\mathbb{Z}} = \mathbb{Z}_{/p_1\mathbb{Z}} \times ... \times \mathbb{Z}_{/p_n\mathbb{Z}}$, solve the linear systems in each field, recompose the solution using CRT and Hensel Lifting.
- Specialized sparse algebra solvers are needed, not trivial.

Coppersmith's Linear Sieve

Factor-base

Take $H = [\sqrt{p}] + 1$ and $J = H^2 - p$.
S=$\{q \ / q \in \ \mathbb{Z} \ prime, \ q \leq L_p[\frac{1}{2}, \frac{1}{2}]\} \cup \{H + c \ / 0 \ < \ c \ < L_p[\frac{1}{2}, \frac{1}{2} + \epsilon]\}$.
S contains the set of small primes, along with integers near H.
$|S| \approx L_p[\frac{1}{2}, \frac{1}{2} + \epsilon]$.

Residues

Find pairs (c_1, c_2) for which
$(H + c_1)(H + c_2) \equiv J + (c_1 + c_2)H + c_1 c_2 \equiv \prod q_i^{k_i} \mod p$ and
$c_1, c_2 \leq L_p[\frac{1}{2}, \frac{1}{2} + \epsilon]\}$. The residue is around $\mathcal{O}(\sqrt{p})$.

Linear relations

$log_g(H + c_1) + log_g(H + c_2) = \sum_i k_i \times log_g q_i \mod p - 1$.

Coppersmith's Linear, cont.

Line by line sieving

Fix c_1 then observe that $p_i/(H + c_1)(H + c_2)$ when $x \equiv -\frac{J+c_1H}{H+c_1} \mod p_1$.

Coppersmith's $\mathbb{Z}[i]$ method

Linear sieve produces very sparse matrixes, in practice we use the $Z[i]$ method, for which we need to find a quadratic extension $\mathbb{Z}[\sqrt{r}]$, with r negative integer, quadratic residue in $\mathbb{Z}_{/p\mathbb{Z}}$.

UFDs

The Gaussian integer sieve cannot be used regardless of the situation, sometimes we need to resort to the linear sieve.

Index Calculus on Hyperelliptic Curves

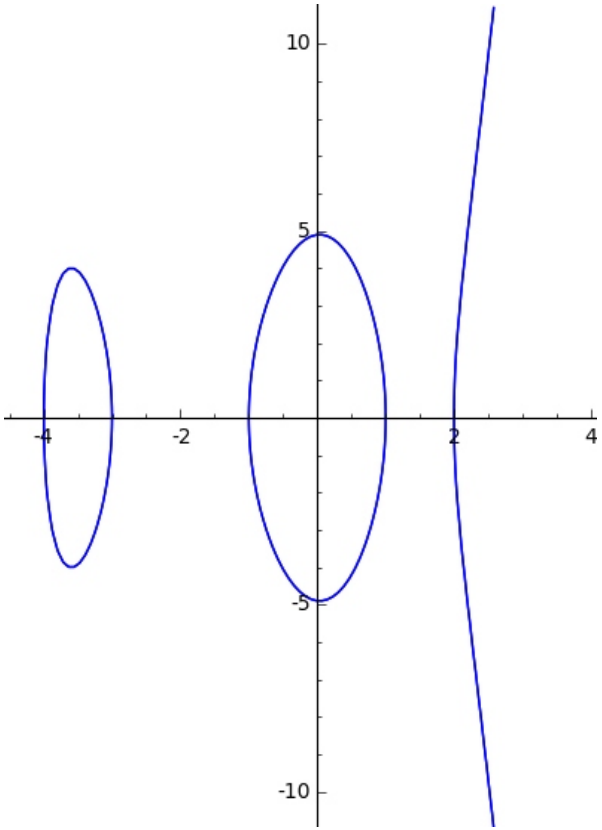

Figure :
$y^2 = x^5 + 5x^4 - 3x^3 - 29x^2 + 2x + 24$, over $\mathbb{R}$

Hyperelliptic Curve

An algebraic curve C, defined over K, given by the equation $C : y^2 + h(x)y = f(x)$ is a hyperelliptic curve of genus g if it is smooth and the polynomials f, h satisfy: $deg(f) = 2g + 1$ and $deg(h) \leq g$.

$C(\mathbb{R})$, $\mathbb{R}-$rational points

Rational points cannot form an abelian group endowed with a geometric law of composition.

Divisors

The divisor group $Div(C)$ of an algebraic curve C is the free abelian group generated by the points of C.
$D \in Div(C) \implies D = \sum_{P \in C} n_p(P)$, $n_p \in \mathbb{Z}$ and $n_p \neq 0$ only for finitely many P.

Linear equivalence $D_1 \sim D_2$ if there exists $f \in \bar{K}(C)$ such that $D_1 = div(f) + D_2$.

Picard's group $Pic(C) = Div(C)/_{\sim}$, and $Pic^0(C) = Div^0(C)/_{\sim}$. $Pic^0_K(C)$ is the subgroup of $Pic^0(C)$ fixed by the Galois action of $Gal(\bar{K}/K)$.

Mumford Representation: Each divisor of degree 0 can be written (eventually) as the polynomial pair $(U(x), V(x))$, where $U(x)$ monic, $U(x)/(f(x) - h(x)V(x) - V(x)^2)$ and $deg(V(x)) < deg(U(x)) \leq g$.

The Jacobian Variety

The Jacobian: $Pic^0(C)$, endowed with the addition for reduced divisors in Mumford representation (Cantor's Algorithm), is an abelian variety $J(C)$, called the Jacobian of C.

HCDLP: Given $D_1, D_2 \in J_{\mathbb{F}_{p^n}}(C)$, we need to find an integer λ, such that $D_2 = \lambda D_1$. Also known is the fact that D_2 belongs to the subgroup generated by D_1, along with the order n of this subgroup.

Automorphisms σ on the hyperelliptic curve transfer to automorphisms on the Jacobian variety. An example for this is the hyperelliptic involution $\omega((a_j, b_j))) = (a_j, -b_j - h(a_j))$. Rho-Pollard can be accelerated by a factor of $\sqrt{ord(\sigma)}$.

Gaudry's Algorithm

Prime divisor: A divisor D, given by its Mumford representation $(U(x), V(x))$, is said to be prime if $U(x)$ is irreducible over $\mathbb{F}_{p^n}$.

A divisor D, given by the pair $(U(x), V(x))$ is said to be $S - smooth$ if all of its prime divisors have the corresponding polynomial $U(x)$ of degree at most S. If $S = 1$, a $1 - smooth$ divisor will have $U(x)$ split completely over $\mathbb{F}_{p^n}$.

Proportion of smooth divisors

The Jacobian of a curve of genus g over $\mathbb{F}_{p^n}$ has a proportion of $\frac{1}{g!}$ $1 - smooth$ divisors when $p^n \to +\infty$.

An Implementation of Gaudry's Algorithm

Zeta function

Consider C to be hyperelliptic of genus g defined over $\mathbb{F}_{p^n}$ and $M_r = J_{\mathbb{F}_{p^{nr}}}(C)$. The zeta function is defined as $Z(C_{/\mathbb{F}_{p^n}}; T) = e^{\sum_{r=1}^{\infty} \frac{M_r T^r}{r}}$.

Algorithm outline

- Perform an additive Rho-Pollard pseudo-random walk $W_i = w_0^1 D_1 + w_0^2 D_2$.
- Test divisors for $1 - smoothness$, decompose smooth divisors to get linear relations of prime divisors.
- Compute an element from the left null-space of the obtained matrix modulo cardinality of $J_{\mathbb{F}_{p^n}}(C)$.
- Use element of the kernel to "compute" $E_i = E_j$ and obtain $\lambda \equiv \frac{e_i^1 - e_j^1}{e_j^2 - e_i^2} \mod |J_{\mathbb{F}_{p^n}}(C)|$.

Conclusions

Main points of the theoretical survey

- Sub-case of the NFS
- Index calculus outline
- Coppersmith's linear sieve
- Coppersmith's Gaussian Integer Method
- Rho-Pollard Improvements for HCC
- Gaudry's algorithm
- Thériault's variant

Practical implementations

- Basic Index Calculus(PARI/GP) + Rho Pollard
- Coppersmith's linear sieve
- Instantiation of convenient genus 2 hyperelliptic curves
- Gaudry's algorithm (SAGE 6.7)

Thank you!

Questions?