Worked Example for the Special Number Field Sieve

Jonathan Bootle

University College London

This document gives a worked example of a discrete logarithm computation using the Special Number Field Sieve algorithm, following a similar strategy to those given in [Gor93] and [Sch93].

1 Goal

Let $p = 1019$, $q = 509$. These are both primes, and $p = 2q + 1$. Let $g = 277$, $h = 487$, so that g generates the subgroup of order q inside $\mathbb{Z}/p\mathbb{Z}$.

Problem Compute x such that $g^x = h \mod p$.

2 Polynomial Choice

First, we will choose a monic polynomial f with small coefficients, which is irreducible over $\mathbb{Q}$. By Gauss' Lemma, it will be sufficient to check irreducibility over $\mathbb{Z}$. A integer polynomial is called primitive if the greatest common divisor of its coefficients is 1.

Theorem 1 (Gauss' Lemma). *A non-constant polynomial in $\mathbb{Z}[X]$ is irreducible in $\mathbb{Z}[X]$ if and only if it is both irreducible in $\mathbb{Q}[X]$ and primitive in $\mathbb{Z}[X]$.*

We choose $d = 2$ and set $m = 31 \approx p^{1/d}$. Next, we produce f of degree d by expressing p in base m, which ensures that none of the coefficients of f are greater than m, and hence quite small modulo p. There are many other methods of producing f using the LLL algorithm and other techniques.

$$p = m^2 + m + 27, \qquad f(X) = X^2 + X + 27$$

We must also check that f is irreducible. Some methods for checking irreducibility over $\mathbb{Z}$ involve changing variables, Eisenstein's Criterion, and brute force. In this case, we are lucky, because $f(m)$ is prime, and we can apply Cohn's Irreducibility Criterion. Otherwise, since f is quadratic, we can simply note that it has no rational roots.

Theorem 2 (Generalisation of Cohn's Irreducibility Criterion). *[Bri] Assume that $m \geq 2$ is a natural number, and $f(X) = a_k X^k + a_{k-1} X^{k-1} + \ldots + a_1 X + a_0$, with $0 \leq a_i \leq m - 1$. If $f(m)$ is a prime number then $f(X)$ is irreducible in $\mathbb{Z}[X]$.*

Also, note that the discriminant of f is -107, which is coprime with q.
The roots of f are given by $\alpha_\pm = \frac{-1\pm\sqrt{-107}}{2}$. Write $\alpha = \alpha_+$.
We use $g(X) = X - m$.

3 Finding the Factor Bases

We set $B = 15$ to be the smoothness bound for both our rational and algebraic factor bases. According to Theorem 3.1.7 in Mathew Brigg's thesis, we have the following correspondence.

Theorem 3. *[Bri98] Let f be a monic, irreducible polynomial with integer coefficients and $\alpha \in \mathbb{C}$ a root of f. The set of pairs (r, p) where p is a prime integer and $r \in \mathbb{Z}/p\mathbb{Z}$ with $f(r) = 0 \mod p$ is in bijective correspondence with the set of all first degree prime ideals of $\mathbb{Z}[\alpha]$.*

Therefore, we store the primes in the rational factor basis in the form $(m \mod p_i, p_i)$, and the primes in the algebraic factor basis in the form (r, p_i) for the roots r that we find.

Our rational factor basis is

$$\{(1, 2), (1, 3), (1, 5), (3, 7), (9, 11), (5, 13)\}$$

To find our algebraic factor basis, we must attempt to factorise f modulo primes less than 15. We discover that f has no roots modulo 2, 5 and 7, so there are no prime ideals of norm 2, 5 or 7. We discover the following roots.

$$f(x) = 0 \mod 3 \text{ for } x = 0, 2 \mod 3$$
$$f(x) = 0 \mod 11 \text{ for } x = 2, 8 \mod 11$$
$$f(x) = 0 \mod 13 \text{ for } x = 3, 9 \mod 13$$

Our algebraic factor basis is

$$\{(0, 3), (2, 3), (2, 11), (8, 11), (3, 13), (9, 13)\}$$

4 Sieving

According to Theorem 3.1.9 in Mathew Brigg's thesis, we have the following correspondence.

Theorem 4. *[Bri98] Given an element $\beta \in \mathbb{Z}[\alpha]$ of the form $\beta = a + b\alpha$ for coprime integers a and b and a prime ideal p of $\mathbb{Z}[\alpha]$, then we have $v_\mathfrak{p}(\beta) = 0$ if $\mathfrak{p}$ is not a first degree prime ideal of $\mathbb{Z}[\alpha]$. Furthermore, if $\mathfrak{p}$ is a first degree prime ideal of $\mathbb{Z}[\alpha]$ corresponding to the pair (r, p) as in Theorem 3.1.7, then $v_\mathfrak{p}(\beta) = v_p(N(\beta))$ if $a = -br \mod p$ and 0 otherwise.*

We proceed by computing $a + bm$ and $N(a + b\alpha)$ for small integers a and b, and checking whether they are smooth. The theorem above gives us information about whether a particular choice of a and b will lead to a useful relation. For example, if a and b are coprime but do not satisfy at least one of the following conditions

$$a = -b \mod 2, \qquad a = -b \mod 3$$

$$a = -b \mod 5, \qquad a = -3b \mod 7$$

$$a = -9b \mod 11, \qquad a = -5b \mod 13$$

then $a + bm$ will not be divisible by any of the primes in the rational factor basis, and we will not obtain a useful relation. Similarly, if a and b are coprime but do not satisfy at least one of the following conditions

$$a = 0 \mod 3, \qquad a = -2b \mod 3$$

$$a = -2b \mod 11, \qquad a = -8b \mod 11$$

$$a = -3b \mod 13, \qquad a = -9b \mod 13$$

then $N(a + b\alpha)$ will not be divisible by 3, 11 or 13, so $(a + b\alpha)$ will not be divisible by any of the prime ideals in the algebraic factor basis.

In order to get a useful relation, a and b must be coprime, and satisfy at least one of the first set of conditions, and at least one of the second set of conditions. Even then, $a + bm$ or $N(a + bm)$ might be divisible by a prime not in the factor basis, and hence might not be B-smooth.

The norm $N(a + b\alpha)$ can be computed as $N(a + b\alpha) = (-b)^d f(-a/b) = a^2 - ab + 27b^2$. In [FGHT16], the authors suggest that it could be advantageous to choose f with at least one real root. Intuitively, one reason for this is that if $-a/b$ is close to a real root of f, then the norm is likely to be small, and perhaps then more likely to be smooth.

In the end, after trying many values of a and b, we end up with the following table of values.

a	b	$a+bm$	$N(a+b\alpha)$	-1	2	3	5	7	11	13	$(0,3)$	$(2,3)$	$(2,11)$	$(8,11)$	$(3,13)$	$(9,13)$
1	-7	-216	1331	1	3	3	0	0	0	0	0	0	0	3	0	0
1	1	32	27	0	5	0	0	0	0	0	0	3	0	0	0	0
1	4	125	429	0	0	0	3	0	0	0	0	1	0	1	1	0
3	-1	-28	39	1	2	0	0	1	0	0	1	0	0	0	1	0
4	1	35	39	0	0	0	1	1	0	0	0	1	0	0	0	1
8	7	225	1331	0	0	2	2	0	0	0	0	0	3	0	0	0
9	-1	-22	117	1	1	0	0	0	1	0	2	0	0	0	0	1
9	1	40	99	0	3	0	1	0	0	0	2	0	1	0	0	0
9	25	784	16731	0	4	0	0	2	0	0	2	0	0	1	0	2
26	-1	-5	729	1	0	0	1	0	0	0	0	6	0	0	0	0
27	-2	-35	891	1	0	0	1	1	0	0	4	0	0	1	0	0
29	2	91	891	0	0	0	0	1	0	1	0	4	1	0	0	0
35	-1	4	1287	0	2	0	0	0	0	0	0	2	1	0	0	1
37	-17	-490	9801	1	1	0	1	2	0	0	0	4	0	2	0	0

5 Schirokauer Maps

Write $\mathcal{O} = \mathbb{Z}[\alpha]$. Let $\Gamma = \{\gamma \in \mathcal{O} : N(\gamma) \neq 0 \mod q\}$. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_k$ be the prime ideals above q. Set $\epsilon_{\mathfrak{q}_j} = \left|(\mathcal{O}/\mathfrak{q}_j)^*\right|$. Set $\epsilon = \operatorname{lcm}\{\epsilon_{\mathfrak{q}_1}, \ldots, \epsilon_{\mathfrak{q}_k}\}$.

Let $\{b_j\}_{j=1}^d$ be a $\mathbb{Z}$-basis for $\mathcal{O}$, so that $\{b_j q + q^2\mathcal{O}\}_{j=1}^d$ is a $\mathbb{Z}/q\mathbb{Z}$-basis for $q\mathcal{O}/q^2\mathcal{O}$. Consider the map

$$\Gamma \to q\mathcal{O}/q^2\mathcal{O}$$

$$\gamma \mapsto (\gamma^\epsilon - 1) + q^2\mathcal{O}$$

Then any $(\gamma^\epsilon - 1) + q^2\mathcal{O}$ can be written as $\sum_{j=1}^d \lambda_j(\gamma) b_j q + q^2\mathcal{O}$. We must compute the values $\lambda_j(\gamma)$ - the Schirokauer maps - for each $\gamma = a + b\alpha$ in the table, and add columns containing these values.

Rationale If the value of each Schirokauer map is equal to zero, then γ is likely to be an lth power in $\mathcal{O}$. See [Sch93] or [Sch08] for more details.

We have $q = 509$, and can find the values of the $\epsilon_{\mathfrak{q}_i}$ for prime ideals $\mathfrak{q}_i$ above q by factorising f modulo q, and applying Dedekind's Criterion.

Theorem 5 (Simplified Version of Dedekind's Criterion). *Let α be a root of the irreducible polynomial $f \in \mathbb{Z}[X]$. Suppose that q does not divide the discriminant of f. If $\bar{f} = f \mod q$ has factorisation into irreducibles $\bar{f} = \prod_{i=1}^r \bar{f}_r^{e_r}$ modulo q, then (q) factors into prime ideals as $\mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r}$, where $\mathfrak{p}_i = (p, \bar{f}_i(\alpha))$.*

See [KCo] for a more precisely stated version with a proof.

We discover that

$$f(X) = (X - 129)(X - 379) \mod q$$

This implies that we have two prime ideals $\mathfrak{q}_1$ and $\mathfrak{q}_2$ above q, with

$$\epsilon_{\mathfrak{q}_1} = \epsilon_{\mathfrak{q}_2} = q - 1$$

Therefore, $\epsilon = q - 1$.

How might we actually compute the Schirokauer maps? Using computer algebra software like SAGE, you can simply set up the ring $\mathbb{Z}[\alpha]$ and do the computation in this ring, modulo $q^2\mathbb{Z}[\alpha]$. If you struggle to think about number rings, or are using a more basic package with only integers and modular arithmetic operations, you might do as follows.

To see how γ^ϵ might be computed, create a matrix M_γ which represents multiplication by γ.

For example, $\{1, \alpha\}$ is a basis for $\mathcal{O}$, and $f(\alpha) = \alpha^2 + \alpha + 27 = 0$. Then

$$(a + b\alpha)(x + y\alpha) = ax - 27by + (ay + bx - by)\alpha$$

We can write this as a linear map.

$$M_\gamma \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & -27b \\ b & a - b \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax - 27by \\ ay + bx - by \end{pmatrix}$$

Now, $(M_\gamma)^\epsilon \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ represents γ^ϵ, so

$$(M_\gamma)^\epsilon \begin{pmatrix} 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

represents $\gamma^\epsilon - 1$. Doing this computation modulo q^2 gives the vector $\begin{pmatrix} \lambda_1(\gamma)q \\ \lambda_2(\gamma)q \end{pmatrix}$ and dividing by q gives the values of the Schirokauer maps.

Following either of these methods allows us to augment our table with the values of the Schirokauer maps.

a	b	$a+bm$	$N(\gamma)$	-1	2	3	5	7	11	13	$(0,3)$	$(2,3)$	$(2,11)$	$(8,11)$	$(3,13)$	$(9,13)$	$\lambda_1(\gamma)$	$\lambda_2(\gamma)$
1	-7	-216	1331	1	3	3	0	0	0	0	0	0	0	3	0	0	422	245
1	1	32	27	0	5	0	0	0	0	0	0	3	0	0	0	0	276	163
1	4	125	429	0	0	0	3	0	0	0	0	1	0	1	1	0	119	197
3	-1	-28	39	1	2	0	0	1	0	0	1	0	0	0	1	0	433	346
4	1	35	39	0	0	0	1	1	0	0	0	1	0	0	0	1	87	163
8	7	225	1331	0	0	2	2	0	0	0	0	0	3	0	0	0	177	264
9	-1	-22	117	1	1	0	0	0	1	0	2	0	0	0	0	1	240	0
9	1	40	99	0	3	0	1	0	0	0	2	0	1	0	0	0	304	149
9	25	784	16731	0	4	0	0	2	0	0	2	0	0	1	0	2	206	360
26	-1	-5	729	1	0	0	1	0	0	0	0	6	0	0	0	0	43	326
27	-2	-35	891	1	0	0	1	1	0	0	4	0	0	1	0	0	461	34
29	2	91	891	0	0	0	0	1	0	1	0	4	1	0	0	0	427	475
35	-1	4	1287	0	2	0	0	0	0	0	0	2	1	0	0	1	238	475
37	-17	-490	9801	1	1	0	1	2	0	0	0	4	0	2	0	0	310	211

6 Linear Algebra

This is a final step, where we try to use the relations that we have collected to compute the discrete logarithm of h with respect to g. We must introduce entries corresponding to h into our table, and create a vector corresponding to g. Unfortunately, neither g nor h is B-smooth.

To fix this, I have chosen random values of R and S which result in $H = g^R h$ and $G = g^S$ which are B-smooth. Now, computing the discrete logarithm of H with respect to G allows us to solve our original problem. For example, taking $R = 187$ and $S = 299$, we have $H = 625 = 5^4$ and $G = 33 = 3 \cdot 11$.

Form a vector $\mathbf{v}_H$ which consists of the exponents used when expressing H in terms of our rational factor basis, with all other entries zero. Do the same for $\mathbf{v}_G$. In this case, we have

$$\mathbf{v}_H = (0, 0, 0, 4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

$$\mathbf{v}_G = (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

Also, create a vector $\mathbf{v}_{a,b}$ corresponding to the entries for the rational factor basis, algebraic factor basis, and λ values for each pair of a and b values in the table. For example

$$\mathbf{v}_{1,-7} = (1, 3, 3, 0, 0, 0, 0, 0, 0, 0, 3, 0, 0, 422, 245)$$

Form the matrix A consisting of columns $\mathbf{v}_G, \mathbf{v}_{1,-7}, \mathbf{v}_{1,1}, \ldots, \mathbf{v}_{37,-17}$. We will then try to find a vector $\mathbf{x}$ which solves the matrix equation $A\mathbf{x} = -\mathbf{v}_H$ modulo q.

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 3 & 5 & 0 & 2 & 0 & 0 & 1 & 3 & 4 & 0 & 0 & 0 & 2 & 1 \\ 1 & 3 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 1 & 2 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 2 & 0 & 1 & 1 & 0 & 2 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 2 & 2 & 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 3 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 6 & 0 & 4 & 2 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 3 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 2 & 0 & 0 & 0 & 1 & 0 \\ 0 & 422 & 276 & 119 & 433 & 87 & 177 & 240 & 304 & 206 & 43 & 461 & 427 & 238 & 310 \\ 0 & 245 & 163 & 197 & 346 & 163 & 264 & 0 & 149 & 360 & 326 & 34 & 475 & 475 & 211 \end{pmatrix} \mathbf{x} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 505 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \mod 509$$

Note The matrix A is relatively sparse, and the most entries are small with respect to q, except for the last two rows. Therefore, special techniques for sparse linear algebra should be used to find $\mathbf{x}$.

We find that

$$\mathbf{x} = (76, 102, 356, 230, 279, 438, 318, 433, 64, 328, 50, 154, 0, 0, 0)$$

is a solution. Hence, it is likely that $H = G^{-76} \mod p$. Substituting in $H = g^R h$ and $G = g^S$, we find that $h = g^{-76S-R \mod q} = g^{503} \mod p$.

References

Bri. *On an irreducibility theorem of a. cohn.* `https://cms.math.ca/openaccess/cjm/v33/cjm1981v33.1055-1059.pdf`. Accessed: 2017-03-17.

Bri98. M. E. Briggs. *An Introduction to the General Number Field Sieve An Introduction to the General Number Field Sieve.* 1998.

FGHT16. J. Fried, P. Gaudry, N. Heninger, and E. Thomé. *A kilobit hidden SNFS discrete logarithm computation. Eprint*, (September):1, 2016.

Gor93. D. Gordon. *Discrete Logarithms in GF(P) Using the Number Field Sieve. SIAM Journal on Discrete Mathematics*, (1):1, 1993.

KCo. *Math 154: Dedekind's factorization criterion.* `http://math.stanford.edu/~conrad/154Page/handouts/dedekindcrit.pdf`. Accessed: 2017-03-17.

Sch93. O. Schirokauer. *Discrete logarithms and local units. ... Transactions of the Royal Society of ...*, 1993.

Sch08. O. Schirokauer. *The impact of the number field sieve on the discrete logarithm problem in finite fields. Algorithmic Number Theory*, 44:397, 2008.