Factoring Integers and Computing Discrete Logarithms via Diophantine Approximation

C. P. Schnorr
Universität Frankfurt
Fachbereich Mathematik/Informatik
6000 Frankfurt am Main
Germany

email: schnorr@informatik.uni-frankfurt.de

Abstract

Let N be an integer with at least two distinct prime factors. We reduce the problem of factoring N to the task of finding random integer solutions $(e_1, \ldots, e_t) \in \mathbb{Z}^t$ of the inequalities

$$\left| \sum_{i=1}^{t} e_i \log p_i - \log N \right| \leq N^{-c} \qquad \text{and}$$

$$\sum_{i=1}^{t} |e_i \log p_i| \leq (2c-1) \log N + o(\log p_t),$$

where $c > 1$ is fixed and $p_1, \ldots, p_t$ are the first t primes. We show, under the assumption that the smooth integers distribute "uniformly", that there are $N^{\varepsilon + o(1)}$ many solutions $(e_1, \ldots, e_t)$ if $c > 1$ and if $\varepsilon := c - 1 - (2c-1) \log \log N / \log p_t > 0$. We associate with the primes $p_1, \ldots, p_t$ a lattice $L \subset \mathbb{R}^{t+1}$ of dimension t and we associate with N a point $\mathbf{N} \in \mathbb{R}^{t+1}$. We reduce the problem of factoring N to the task of finding random lattice vectors $\mathbf{z}$ that are sufficiently close to $\mathbf{N}$ in both the ∞-norm and the 1-norm. The dimension t of the lattice L is polynomial in $\log N$. For $N \approx 2^{512}$ it is about 6300. We also reduce the problem of computing, for a prime N, discrete logarithms of the units in $\mathbb{Z}_{/N\mathbb{Z}}$ to a similar diophantine approximation problem.

D.W. Davies (Ed.): Advances in Cryptology - EUROCRYPT '91, LNCS 547, pp. 281-293, 1991.

1 Summary

The task of factoring large composite integers N has a long history and is still a challenging problem. In this paper we reduce this task to the following problem of diophantine approximation. Find about $t+2$ integer vectors $(e_1, \ldots, e_t) \in \mathbb{Z}^t$ so that $|\sum_{i=1}^{t} e_i \log p_i - \log N| \leq N^{-c}$ and $\sum_{i=1}^{t} |e_i \log p_i| \leq (2c-1)\log N + o(\log p_t)$ hold for some $c > 1$ where $p_1, \ldots, p_t$ are the first t prime numbers.

Given these $t+2$ diophantine approximations of $\log N$ we can factorize N as follows. The integer $u := \prod_{e_j>0} p_j^{e_j}$ must be a close approximation to vN where $v = \prod_{e_j<0} p_j^{|e_j|}$. In fact we show in Lemma 2 that $|u - vN| = p_t^{o(1)}$. Hence the residue $u \pmod N$ factorizes completely over the primes $p_1, \ldots, p_t$ and we obtain a non trivial congruence $\prod_{e_j>0} p_j^{e_j} = \pm \prod_{j=1}^{t} p_j^{b_j} \pmod N$. Using about $t+2$ of these congruences we can factorize N according to the method in section 2.

The above diophantine approximation problem can be formulated as a closest lattice vector problem. In section 3 we associate with N a point $\mathbf{N} \in \mathbb{R}^{t+1}$ and with the primes $p_1, \ldots, p_t$ a lattice L so that the desired approximations $\sum_{i=1}^{t} e_i \log p_i$ of $\log N$ can be generated from the lattice vectors $\mathbf{z}$ such that $\|\mathbf{z}-\mathbf{N}\|_1$ and $\|\mathbf{z}-\mathbf{N}\|_\infty$ are sufficiently small. We show in Lemma 2 that every lattice vector that is sufficiently close to $\mathbf{N}$ yields a desired approximation of $\log N$. Under a reasonable hypothesis we show in Theorem 7 that, for some fixed $\varepsilon > 0$, there are at least $N^{\varepsilon+o(1)}$ sufficiently close lattice vectors provided that the number t of primes is larger than $(\log N)^2$. These results reduce the problem of factoring N to the task of finding lattice vectors in L that are close to $\mathbf{N}$ in both the 1–norm and the ∞–norm.

The lattice basis reduction algorithm of Lenstra, Lenstra, Lovász (1982) apparently let some experts think on the possibility to factorize N by finding good approximations to N by a linear combination of log's of small primes. Since this approach seemed to be impractical it has never been analysed. We introduce negative coefficients into the approximation problem and we set up this problem as a nearest lattice vector problem. We also obtain explicit numbers on the size of the lattice and error bounds needed to make the method work.

We have solved the diophantine approximation problem using a prime basis of $t = 125$ primes. We reduce the lattice basis by blockwise Korkine Zolotarev reduction, a concept that has been introduced by Schnorr (1987). Schnorr and Euchner (1991) give improved practical algorithms for lattice basis reduction. For a basis of 125 primes the diophantine approximation problem can be solved

within a few hours on a SPARC 1+ computer. In general it may be hard to find a lattice vector that is very close in both the 1–norm and the ∞–norm. Our experience with the particular problem indicates that it is sufficient to reduce by a strong reduction algorithm for the Euclidean norm, the lattice basis $b_1, \ldots, b_t$,N described in section 3. In order to factor integers N that are 500 bits long the basis should have about 6300 primes. It is difficult to estimate the required computer time.

The paper is organized as follows. In section 2 we show how to factor N if we are given about $t+2$ pairs of integers (u_i, v_i) such that u_i is of the form $\prod_{j=1}^{t} p_j^{a_j}$ and $|u_i - v_i N| \leq p_t$. In section 3 we show that these pairs (u_i, v_i) can be generated from the lattice vectors in the lattice L that is associated with the primes $p_1, \ldots, p_t$ that are sufficiently close to the point N We show in section 4 that there are $N^{\epsilon+o(1)}$ lattice vectors that are sufficiently close to N. In section 5 we reduce the problem of computing discrete logarithms to the task of solving a closest lattice vector problem in an associated lattice.

2 Factoring integers via smooth numbers

Notation Let $\mathbb{N}, \mathbb{Q}, \mathbb{R}$ be the sets of natural, integer, real numbers. Let $\log x$ denote the natural logarithm of $x \in \mathbb{R}, x > 0$.

The factoring method

Input. N (a composite integer with at least two distinct prime factors and α, c with $\alpha, c > 1$. The choice for α, c is discussed in section 3)

1. Form the list $p_1, \ldots, p_t$ of all primes smaller than $(\log N)^{\alpha}$.
2. Generate from lattice vectors, as explained in section 3, a list of $m \geq t+2$ pairs $(u_i, v_i) \in \mathbb{N}^2$ with the property that

$$u_i = \prod_{j=1}^{t} p_j^{a_{i,j}} \quad \text{with } a_{i,j} \in \mathbb{N} \tag{1}$$

$$|u_i - v_i N| \leq p_t \tag{2}$$

3. Factorize $u_i - v_i N$ for $i = 1, \ldots, m$ over the primes $p_1, \ldots, p_t$ and $p_0 = -1$. Let $u_i - v_i N = \prod_{j=0}^{t} p_j^{b_{i,j}}$, $\mathbf{b}_i = (b_{i,0}, \ldots, b_{i,t})$ and $\mathbf{a}_i = (a_{i,0}, \ldots, a_{i,t})$ with $a_{i,0} = 0$.

4. Find a nonzero 0,1-solution $(c_1, \ldots, c_m)$ of the equation

$$\sum_{i=1}^{m} c_i(\mathbf{a}_i - \mathbf{b}_i) = 0 \ (\mathrm{mod} 2)$$

5. $$x := \prod_{j=0}^{t} p_j^{\sum_{i=1}^{m} c_i(a_{i,j}+b_{i,j})/2} \ (\mathrm{mod} N) \ ,$$

$$y := \prod_{j=0}^{t} p_j^{\sum_{i=1}^{m} c_i b_{i,j}} = \prod_{j=1}^{m} u_i^{c_i} (\mathrm{mod} N) \ .$$

(The construction implies that $x^2 = y^2 (\mathrm{mod} N)$.)

6. If $x \neq \pm y (\mathrm{mod} N)$ then *output* $gcd(x+y, N)$ and stop. Otherwise go to 4 and generate a different solution $(c_1, \ldots, c_m)$.

Remarks. 1. If x, y in step 5 behave like a random solution of $x^2 = y^2 (\mathrm{mod}$ $N)$ then the success rate of step 6 is at least $1/2$. Therefore the time that the algorithm takes to factorize N is essentially the time to generate the list of $m \geq t+2$ pairs (u_i, v_i) required in step 2.
2. Steps 4 – 6 of the algorithm only require that u_i and $u_i (\mathrm{mod}\, N)$ factorize completely over the prime basis $p_1, \ldots, p_t$. In case of the weaker inequality $|u_i - v_i N| = p_t^{O(1)}$ we expect that $u_i - v_i N$ factorizes completely over the prime basis for at least some fixed positive fraction of the pairs (u_i, v_i).
3. In the next section we introduce a lattice $L_{\alpha,c}$ and we show that essentially every vector in $L_{\alpha,c}$ that is sufficiently close to the point $\mathbf{N}$ yields some pair $(u_i, v_i) \in \mathbb{N}^2$ such that (1), (2) hold. Moreover assuming an unproved but reasonable hypothesis we show that if $\alpha > (2c-1)/(c-1)$ then the lattice vectors that are close to $\mathbf{N}$ yield sufficiently many suitable pairs (u_i, v_i) satisfying (1) and (2).
4. By the prime number theorem the number t of primes $\leq (\log N)^\alpha$ is

$$t = (\log N)^\alpha \, / \, \alpha \log\log N \ (1 + o(1)) \ .$$

3 How to generate $\mathbf{u_i, v_i}$ from lattice vectors that are close to N

Let $L = L_{\alpha,c} \subset \mathbb{R}^{t+1}$ be the lattice that is generated by the column vectors $\mathbf{b}_1, \ldots, \mathbf{b}_t$ of the following $(t+1) \times t$ matrix B and let $\mathbf{N} \in \mathbb{R}^{t+1}$ be represented

by the following column vector:

$$B = \begin{bmatrix} \log 2 & 0 & \cdots & 0 \\ 0 & \log 3 & & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \log p_t \\ N^c \log 2, & N^c \log 3 & \cdots & N^c \log p_t, \end{bmatrix} \qquad \mathbf{N} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ N^c \log N \end{bmatrix}$$

We let the rational numbers $\alpha, c > 1$ vary only slightly with the size of N. The real entries of the matrix B must be approximated by rational numbers. We show below that it is sufficient to approximate them with an error less than $1/2$, i.e. we can approximate them by the nearest integer.

Notation. We associate with a lattice vector $\mathbf{z} = (z_1, \ldots, z_{t+1}) = \sum_{i=1}^{t} e_i \mathbf{b}_i$, $e_1, \ldots, e_t \in \mathbb{Z}$, the pair of integers $g(\mathbf{z}) := (u, v) \in \mathbb{N}^2$ with

$$u := \prod_{e_j > 0} p_j^{e_j}, \quad v := \prod_{e_j < 0} p_j^{|e_j|}.$$

The *maximum norm* of a vector $\mathbf{z} = (z_1, \ldots, z_{t+1}) \in \mathbb{R}^{t+1}$ is by definition $\|\mathbf{z}\|_\infty = \max_i |z_i|$; the *1-norm* is $\|\mathbf{z}\|_1 = \sum_{i=1}^{t+1} |z_i|$. We call an integer $\pm \prod_{i=1}^{t} p_i^{e_i}$ *γ-smooth* if $p_i^{e_i} \leq \gamma$ for $i = 1, \ldots, t$. A pair (u, v) of integers is *γ-smooth* if both u and v are γ-smooth.

Lemma 1. *If $\mathbf{z} \in L$ and $\|\mathbf{z} - \mathbf{N}\|_\infty \leq \log p_t$ then $(u, v) = g(\mathbf{z})$ is p_t-smooth.*

Proof. Let $\mathbf{z} = \sum_{i=1}^{t} e_i \mathbf{b}_i$. We have $|e_i \log p_i| = \log p_i^{|e_i|} \leq \log p_t$ for $i = 1, \cdots, t$. **QED**

For any lattice vector $\mathbf{z} = (z_1, \ldots, z_{t+1}) = \sum_{i=1}^{t} e_i \mathbf{b}_i$ with $(u, v) = g(\mathbf{z})$ we have

$$\|\mathbf{z} - \mathbf{N}\|_1 = \log u + \log v + N^c |\log(u/vN)|. \tag{3}$$

$$z_{t+1} = N^c \log(u/v) \tag{4}$$

Lemma 2. *If $\mathbf{z} \in L$ satisfies the inequalities*

$$\|\mathbf{z} - \mathbf{N}\|_\infty \leq \log p_t \tag{5}$$

$$\|\mathbf{z} - \mathbf{N}\|_1 \leq (2c - 1) \log N + o(\log p_t) \tag{6}$$

then we have for $(u, v) := g(\mathbf{z})$ that $|u - vN| = p_t^{o(1)}$. The asymptotic is for $N \to \infty$.

We see from Fact 1 and Lemma 2 that if $\mathbf{z} \in L$ satisfies (5) and (6) for sufficiently large N then the pair $(u, v) = g(\mathbf{z})$ satisfies the conditions (1), (2) in step 2 of the factoring algorithm.

Proof. We let β denote $z_{t+1} - N^c \log N$, i.e. $\beta = (\mathbf{z} - \mathbf{N})_{t+1}$. From the inequality (5) we only use that $|\beta| \leq \log p_t$. We see from (4) and (5) that

$$\left|\log\left(1 + \frac{u - vN}{vN}\right)\right| = |\log(u/vN)| \overset{(4)}{=} N^{-c}\beta \overset{(5)}{\leq} N^{-c} \log p_t = o(1).$$

Using that $\log(1 + x) = x + o(1)$ for small x this yields

$$|u - vN| \leq vN^{1-c} \log p_t (1 + o(1))$$

Since $\log p_t = p_t^{o(1)}$ it remains to show that $v \leq N^{c-1} p_t^{o(1)}$. We have

$$\begin{aligned} \log v &\overset{(3)}{=} \|\mathbf{z} - \mathbf{N}\|_1 - \log u - |\beta| \\ &\overset{(4)}{=} \|\mathbf{z} - \mathbf{N}\|_1 - \log vN - \beta N^{-c} - |\beta| \\ &\leq \|\mathbf{z} - \mathbf{N}\|_1 - \log vN. \end{aligned}$$

By (6) this implies $2 \log v \leq 2(c-1) \log N + o(\log p_t)$, and thus $v \leq N^{c-1} p_t^{o(1)}$. **QED**

If we replace in Lemma 2 the inequality (6) by the weaker bound

$$\|\mathbf{z} - \mathbf{N}\|_1 \leq (2c - 1) \log N + O(\log p_t)$$

it follows that $|u - vN| = p_t^{O(1)}$. This latter inequality is still sufficient for our factoring method.

Lemma 3. *In the proof of Lemma 2 we have used from the inequalities (5), (6) only that*

$$\left|\sum_{i=1}^{t} e_i \log p_i - \log N\right| \leq N^{-c} \log p_t \tag{7}$$

$$\sum_{i=1}^{t} |e_i \log p_i| \leq (2c - 1) \log N + o(\log p_t) \tag{8}$$

Therefore in order to find an integer pair (u, v) for our factoring method it is sufficient to solve the inequalities (7), (8) with $e_1, \ldots, e_t \in \mathbb{Z}$. The factor $\log p_t$ in (7) is negligible. It can be eliminated by replacing c by $c' = c - \log\log p_t / \log N$. This substitution does not affect the inequality (8) since $\log\log p_t = o(\log p_t)$.

Rational approximation of the basis matrix. In practice we must approximate the real entries of the basis matrix $B = [\mathbf{b}_1, \ldots, \mathbf{b}_t]$ by rational vectors $\overline{\mathbf{b}}_1, \ldots, \overline{\mathbf{b}}_t$. The approximation must be sufficiently close so that the error in $|z_{t+1}|\, N^{-c}$ for $\mathbf{z} = \sum_{i=1}^{t} e_i\, \mathbf{b}_i$ is negligible whenever $|e_i \log p_i| \leq \log p_t$ for $i = 1, \ldots, t$. For this it is sufficient to approximate $N^c \log p_i$, $N^c \log N$, $\log p_i$ by the nearest integer. Then the bit length of $N^c \log p_i$, $N^c \log N$ is $c \log_2 N$ and the bit length of $\log p_i$ is $\log_2 p_t$. If we choose for N^c a power of 2 (10, resp.) then $N^c \log p_i$, $N^c \log N$ is the initial segment of the binary (digital, resp.) representation of $\log p_i$, $\log N$ shifted to the right of the point.

4 There are sufficiently many lattice vectors that are close to N

We show under a reasonable hypothesis that at least $N^{\varepsilon + o(1)}$ lattice vectors $\mathbf{z} \in L$ satisfy the inequalities (5), (6) of Lemma 2 for $\varepsilon = c - 1 - (2c - 1)\log\log N / \log p_t$. Therefore we can factorize N efficiently if $\varepsilon > 0$ and if we can efficiently generate random lattice vectors $\mathbf{z} \in L$ satisfying (5) and (6).

Our argument showing the existence of suitable lattice vectors $\mathbf{z} \in L$ is not constructive. We derive these lattice vectors from smooth integers u, v satisfying $|u - vN| = O(1)$. The existence of these smooth integers follows from the assumption that the smooth integers distribute "uniformly".

Let $\mathbb{N}_t$ denote the set of integers that factorize completely over the primes $p_1, \ldots, p_t$. For $u = \Pi_i p_i^{e_i}$, $v = \Pi_i p_i^{e_i'} \in \mathbb{N}_t$ let $f(u, v) = \sum_{i=1}^{t} (e_i - e_i')\mathbf{b}_i$. The mapping $f : \mathbb{N}_t \times \mathbb{N}_t \to L$ is inverse to g, i.e. $fgf = f$. f is not one–one since we have $f(u, v) = f(uw, vw)$ for all $w \in \mathbb{N}_t$. At most one preimage (u, v) of each $\mathbf{z} \in f(\mathbb{N}_t^2)$ can be used in step 2 of the factoring algorithm. We can always use the minimal preimage $(u, v) = g(\mathbf{z})$.

Lemma 4. *If* $u, v \in \mathbb{N}_t$, $|u - vN| = o(\log p_t)$ *and* $v = \Theta(N^{c-1})$ *then* $\mathbf{z} = f(u, v)$ *satisfies* $\|\mathbf{z} - \mathbf{N}\|_1 \leq (2c - 1)\log N + o(\log p_t)$ *and* $|(\mathbf{z} - \mathbf{N})_{t+1}| = o(\log p_t)$.

Proof. Let $\mathbf{z} = (z_1, \ldots, z_{t+1}) = \sum_{i=1}^{t} e_i \mathbf{b}_i$. We put $\beta := (\mathbf{z} - \mathbf{N})_{t+1} = z_{t+1} - N^c \log N$. We have by (4) $|\beta| N^c |\log(u/vN)| = N^c |\log\left(1 + \frac{u-vN}{vN}\right)| \leq N^c \frac{|u-vN|}{vN} + O(N^c((\log p_t)/vN)^2)$.
It follows from $N^{c-1} = O(v)$, $|u - vN| = o(\log p_t)$ that $|\beta| = o(\log p_t)$. From this and $v = \Theta(N^{c-1})$ we see that

$$\|\mathbf{z} - \mathbf{N}\|_1 \overset{(3)}{=} \log u + \log v + |\beta| \overset{(4)}{\leq} \log v^2 N + |\beta|(1 + N^{-c})$$

$$\leq (2c-1)\log N + o(\log p_t).$$

$$|(\mathbf{z} - \mathbf{N})_{t+1}| = |\beta| = o(\log p_t).$$

QED

We put $p_t = (\log N)^\alpha$, $\log p_t = \alpha \log\log N$. In order to estimate the number of pairs $(u, v) \in \mathbb{N}_t^2$ with $|u - vN| \leq \alpha \log\log N$ we will assume the following

Hypothesis. *The fraction of pairs* (u, v) *in* $\{(u, v) \in \mathbb{N}^2 \mid N^{c-1}/2 < v < N^{c-1}, |u - vN| \leq \alpha \log\log N\}$ *for which* u *and* v *are* $(\log N)^\alpha$*-smooth is at least* $1/(\log N)^{O(1)}$*-times as large as the probability that a random pair in* $\{(u, v) \in \mathbb{N}^2 \mid u \leq N^c,\ v \leq N^{c-1}\}$ *is* $(\log N)^\alpha$*-smooth in* u *and* v.

Theorem 5. (Norton 1971 and Canfield, Erdös, Pomerance, 1983)
Let $\varepsilon > 0$ *be fixed, let* r *satisfy* $N^{1/r} \geq (\log N)^{1+\varepsilon}$. *Then* $\#\{x \leq N \mid x$ *is free of primes* $> N^{1/r}\} / N = r^{-r+o(r)}$ *where* $\lim_{N\to\infty} o(r)/r = 0$.

Remark The proof of Theorem 5 also shows that
$\#\{x \leq N \mid x$ is free of prime powers $p^e > N^{1/r}\}/N = r^{-r+o(r)}$
where $\lim_{N\to\infty} o(r)/r = 0$ provided that $N^{1/r} \geq (\log N)^{1+\varepsilon}$, with $\varepsilon > 0$ fixed.

Let

$$M_{\alpha,c,N} = \left\{ (u, v) \in \mathbb{N}^2 \;\middle|\; \begin{array}{l} |u - vN| \leq \alpha \log\log N \\ N^{c-1}/2 < v < N^{c-1},\ u, v\ (\log N)^\alpha - \text{smooth} \end{array} \right\}$$

Proposition 6. *If the hypothesis holds,* $c > 1$ *and* $\alpha > (2c-1)/(c-1)$ *are fixed then we have* $\#M_{\alpha,c,N} \geq N^{\varepsilon+o(1)}$ *with* $\varepsilon = (c-1) - (2c-1)/\alpha$ *where* $\lim_{N\to\infty} o(1) = 0$.

Proof. Let $r = \log N / \alpha \log\log N$, and thus $(\log N)^\alpha = N^{1/r}$. By the hypothesis, Theorem 5 and the remark we have for sufficiently large N and $\alpha > 1$ that

$$\# M_{\alpha,c,N} \geq N^{c-1} [r(c-1)]^{-r(c-1)} cr^{-cr+o(r)} / (\log N)^{O(1)}.$$

Hence

$$\begin{aligned}
&\log \# M_{\alpha,c,N} \\
&\quad \geq \quad (c-1)\log N - \tfrac{\log N}{\alpha \log\log N}\left((c-1)\log[r(c-1)] + c\log cr\right) \\
&\qquad\quad +o(r\log cr) \\
&\quad \overset{cr \leq \log N}{\geq} \quad [(c-1) - (2c-1)\alpha^{-1}]\log N + o(\log N) \\
&\quad \geq \quad (\varepsilon + o(1))\log N \quad \text{with} \quad \varepsilon = (c-1) - (2c-1)\alpha^{-1}.
\end{aligned}$$

Hence $\# M_{\alpha,c,N} \geq N^{\varepsilon+o(1)}$. **QED**

Theorem 7. *If the hypothesis holds there are $N^{\varepsilon+o(1)}$ many vectors $z \in L$ that satisfy the inequalities (5) and (6), where $\varepsilon = (c-1) - (2c-1)/\alpha$.*

Proof. By Lemma 4 the number of vectors $z \in L$ that satisfy (5), (6) is at least $\# f(M_{\alpha,c,N})$. It will be sufficient to show for all $z \in L$ the inequality

$$\# f^{-1}(z) \cap M_{\alpha,c,N} \leq \alpha \log\log N = N^{o(1)}$$

This inequality and Proposition 6 implies the claim:

$$\# f(M_{\alpha,c,N}) \geq \# M_{\alpha,c,N} / N^{o(1)} = N^{\varepsilon+o(1)}.$$

For any $z \in f(M_{\alpha,c,N})$ there exists $(u,v) \in M_{\alpha,c,N}$ with $f(u,v) = z$ and $gcd(u,v) = 1$. We get (u,v) from any preimage $(\overline{u},\overline{v}) \in f^{-1}(z)$ by dividing both u and v by $gcd(u,v)$. The pair (u,v) is the "minimal" preimage of z and any preimage $(\overline{u},\overline{v}) \in f^{-1}(z)$ is of the form $(\overline{u},\overline{v}) = (uw, vw)$ with $w \in \mathbb{N}_+$. We have $w \mid (\overline{u} - \overline{v}N)$. Since $|\overline{u} - \overline{v}N| \leq \alpha \log\log N$ holds for all $(\overline{u},\overline{v}) \in M_{\alpha,c,N}$ we see that $w \leq \alpha \log\log N$. The desired upper bound on $\# f^{-1}(z) \cap M_{\alpha,c,N}$ follows from $w \leq \alpha \log\log N$. **QED**

Conclusion. We have reduced, by the algorithm in section 2, Lemma 2 and Theorem 7, the problem of factoring N to the problem of finding a random solution $(e_1, \ldots, e_t)$ of the inequalities (7), (8) (to the problem of finding random lattice vectors z satisfying (5), (6), resp.). Our reduction is polynomial time. Its correctness uses two heuristic arguments. First, we assume that $x \not\equiv \pm y \pmod N$ holds with positive probability for the solution of the congruence $x^2 = y^2 \pmod N$ that generated by the algorithm. Second, we assume in the hypothesis that the set of smooth integers is somewhat "uniformly" distributed.

The condition $\alpha > (2c-1)/(c-1)$ in Proposition 6 can be relaxed for small N. We give some examples of parameters α, c so that $\#M_{\alpha,c,N}$ is larger than t.

A scenario for factoring $N \approx 2^{512}$

Let $c = 3$, $\alpha = 1.9$. Hence $(\log N)^\alpha = 70013$, $t \approx (\log N)^\alpha / \alpha \log\log N \approx 6276$ and $r = \log N / \alpha \log\log N \approx 31.8$.
We have

$$\begin{aligned} \log \#M_{\alpha,c,N} &\approx (c-1)\log N - r(c-1)\log r(c-1) - rc\log rc \\ &\geq 710 - 264.3 - 435.2 \\ &\geq 10.5 > \log t \approx 8.75 \end{aligned}$$

At present this seems to be a formidable task. So far we have no experience with lattice basis reduction for lattices with dimension 6300. Moreover the bit length of the input vectors is at least 1500 and a substantial part of the arithmetic has to be done with 1500 precision bits. On the other hand congruences can be constructed within only a few hours computation time in case of dimension 125.

Example solutions of the inequalities (7), (8) using a basis of 125 primes.

Using $t = 125$ primes with the largest prime $p_t = 691$ we have solved the inequalities (7), (8) ((1), (2), resp.) using variants of the LLL-algorithm. Simple LLL-reduction did not generate any solution of the inequalities (7), (8) for this N. We have reduced the lattice basis B of section 3 with 4 precision bits to the right of the point using blockwise Korkine Zolotarev reduction with block size 32. The general concept of blockwise Korkine Zolotarev reduction has been developped in SCHNORR (1987). SCHNIORR and EUCHNER (1991) give practical algorithms and evaluate their performance in solving subset sum problems. For $N = 2131438662079$, $N^c = 10^{25}$, $c \approx 2.03$ we have found the following solutions:

1. $u = 2^4 \cdot 11 \cdot 29 \cdot 37^2 \cdot 43 \cdot 61^2 \cdot 71 \cdot 79 \cdot 97 \cdot 107 \cdot 139 \cdot 167 \cdot 211$
   $v = 5^3 \cdot 7 \cdot 41^2 \cdot 53^2 \cdot 683$, $u - vN = 69$.
   The vector $\mathbf{z} = f(u,v)$ satisfies $\|\mathbf{z}-\mathbf{N}\|_1 \approx 95.88 \approx (2c-1)\log N + 9.19$.

2. $u = 2^4 \cdot 11 \cdot 31^2 \cdot 37 \cdot 61 \cdot 73 \cdot 97 \cdot 107 \cdot 113 \cdot 127 \cdot 149 \cdot 163 \cdot 241 \cdot 257$
   $v = 5^2 \cdot 7^2 \cdot 43 \cdot 47 \cdot 59 \cdot 67 \cdot 83 \cdot 173 \cdot 271$, $u - vN = 29 \cdot 137$.
   The vector $\mathbf{z} = f(u,v)$ satisfies $\|\mathbf{z}-\mathbf{N}\|_1 \approx 102.5 \approx (2c-1)\log N + 15.81$.

3. $u = 3^4 \cdot 5^3 \cdot 11^2 \cdot 17 \cdot 19 \cdot 61 \cdot 67 \cdot 73 \cdot 109 \cdot 193 \cdot 211 \cdot 263$
   $v = 2 \cdot 59 \cdot 101 \cdot 127 \cdot 163 \cdot 173 \cdot 353$, $u - vN = 7$.
   The vector $\mathbf{z} = f(u, v)$ satisfies $\|\mathbf{z} - \mathbf{N}\|_1 \approx 91$.

4. $u = 3 \cdot 19 \cdot 47 \cdot 67 \cdot 71 \cdot 97 \cdot 113 \cdot 151 \cdot 157 \cdot 199 \cdot 239 \cdot 269 \cdot 359$
   $v = 17 \cdot 31 \cdot 107 \cdot 137 \cdot 211 \cdot 223 \cdot 373$, $u - vN = 166$.
   The vector $\mathbf{z} = f(u, v)$ satisfies $\|\mathbf{z} - \mathbf{N}\|_1 \approx 99$

5. $u = 3^3 \cdot 13 \cdot 23 \cdot 31 \cdot 43 \cdot 47 \cdot 101 \cdot 103 \cdot 107 \cdot 173 \cdot 239 \cdot 251 \cdot 283 \cdot 401$
   $v = 2 \cdot 7 \cdot 17 \cdot 29 \cdot 59 \cdot 61 \cdot 89 \cdot 223 \cdot 631$, $u - vN = 139$.
   The vector $\mathbf{z}$ satisfies $\|\mathbf{z} - \mathbf{N}\|_1 \approx 97$.

Note that in our example solutions we have $\|\mathbf{z}-\mathbf{N}\|_1 \approx (2c-1)\log N + 2\log|u - vN|$.

5 Computing discrete logarithms

We reduce the problem of computing discrete logarithms in $\mathbb{Z}_N^*$ to the closest vector problem in an associated lattice L. The dimension of L is polynomial in $\log N$.

Let N be a prime and let $z \in \mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$ be a primitive root of the subgroup of units $\mathbb{Z}_N^* \subset \mathbb{Z}_N$. The logarithm of $y \in \mathbb{Z}_N^*$ to base z, denoted as $\log_z(y)$, is the number $x \in \mathbb{Z}_{N-1}$ satisfying $y = z^x (\mathrm{mod} N)$.

Let $p_1, \ldots, p_t$ be the t smallest prime numbers and let $p_0 = -1$. We can compute $\log_z(y)$ and $\log_z(p_i)$ for $i = 0, \ldots, t$ if we are given $m > t + 2$ general congruences of the form

$$\prod_{j=1}^{t} p_j^{a_{i,j}} \; z^{a_{i,t+1}} \; y^{a_{i,t+2}} \;=\; \prod_{j=0}^{t} p_j^{b_{i,j}} (\mathrm{mod}\, N) \text{ for } i = 1 \ldots m \tag{9}$$

with $a_{i,j}$, $b_{i,j} \in \mathbb{N}$. These congruences can be written as

$$\sum_{j=0}^{t} (a_{i,j} - b_{i,j}) \log_z(p_j) + a_{i,t+1} + a_{i,t+2} \log_z(y) = 0 (\mathrm{mod} N - 1)$$

This is a system of m linear equations in the $t + 2$ unknowns $\log_z(p_j)$ $j = 0, \ldots, t$, $\log_z(y)$. If we have $t + 2$ linearly independent equations then we can determine these unknowns by solving these equations modulo $N - 1$.

The congruences (9) can be obtained from vectors in the following lattice $L = L_{\alpha,c,z,y} \subset \mathbb{R}^{t+3}$ that are $\| \ \|_1$–close to the vector $\mathbf{N}$. The lattice L is generated by the column vectors $\mathbf{b}_1, \ldots, \mathbf{b}_{t+2}$ of the following $(t+3) \times (t+2)$ matrix and $\mathbf{N} \in \mathbb{R}^{t+3}$ is the following column vector.

$$\begin{bmatrix} \log 2 & 0 & \cdots & & 0 \\ 0 & \log 3 & & & \\ & & \ddots & & \vdots \\ \vdots & \vdots & & \log p_t & \vdots \\ & & & & \log y \\ 0 & 0 & & & \log z \\ N^c \log 2 & N^c \log 3 & \cdots & \cdots \quad \cdots & N^c \log z \end{bmatrix} \qquad \mathbf{N} = \begin{bmatrix} 0 \\ \\ \vdots \\ \vdots \\ \\ 0 \\ N^c \log N \end{bmatrix}$$

We associate with a lattice vector $\mathbf{z} = (z_1, \ldots, z_{t+3}) = \sum_{i=1}^{t+2} e_i \, \mathbf{b}_i$ the integer $u = \prod p_j^{e_j}$ where j ranges over the set of indices $j \leq t+2$ with $e_j > 0$ and where $p_{t+1} = y$, $p_{t+2} = z$. If the residue $u (\mathrm{mod}\, N)$ factorizes completely over the basis $p_0 = -1, p_1, \ldots, p_t$ this yields a congruence

$$\prod_{e_j > 0} p_j^{e_j} = \prod_{j=0}^{t} p_j^{b_j} \ (\mathrm{mod} N)$$

as in (9).

Conclusion. Computing the discrete logarithm in $\mathbb{Z}_N^*$ via closest lattice vectors takes about the same time as factoring, via closest lattice vectors, integers having the same length as N.

References

E.R. CANFIELD, P. ERDÖS, C. POMERANCE: *On a problem of Oppenheim concerning "Factorisatio Numerorum"*. J. Number Theory 17, (1983), pp. 1 – 28.

M.J. COSTER, B.A. LMACCHIA, A.M. ODLYZKO and C.P. SCHNORR: *An Improved low-density subset sum algorithm.* Proceedings EUROCRYPT'91. Springer LNCS.

R. KANNAN: *Minkowski's convex body theorem and integer programming.* Math. Oper. Res. 12 (1987), pp. 415 – 440.

J.C. LAGARIAS, H.W. LENSTRA, JR. and C.P. SCHNORR: *Korkin–Zolotarev bases and successive minima of a lattice and its reciprocal lattice.* To appear in Combinatorica.

A.K. LENSTRA, H.W. LENSTRA, JR. AND L. LOVÁSZ: *Factoring polynomials with rational coefficients.* Math. Annalen 261, (1982), pp. 515–534.

K.K. NORTON: *Numbers with small prime factors, and the least kth power non–residue.* Memoirs of the AMS, 106 (1971) 106 pages.

C.P. SCHNORR: *A hierarchy of polynomial time lattice basis reduction algorithms.* Theoret. Comp. Sci. 53, (1987), pp. 201 – 224.

C.P. SCHNORR: *A more efficient algorithm for lattice basis reduction.* Journal of Algorithms 9, (1988), pp. 47 – 62.

C.P. SCHNORR and M. EUCHNER: *Lattice basis reduction: improved practical algorithms and solving subset sum problems.* Proceedings of FCT–symposium 1991, Altenhof near Berlin, Germany, September – To appear in Springer LNCS.