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

March 15, 1993

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 $t+2$ integer solutions $(e_1,\ldots,e_t) \in \mathbb{Z}^t$ of the inequalities

$$\left| \sum_{i=1}^{t} e_i \log p_i - \log N \right| \le N^{-c}\ p_t^{o(1)}$$

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

where $c > 1$ is fixed and $p_1,\ldots,p_t$ are the first t primes. We show, under a reasonable hypothesis, that there are $N^{\varepsilon+o(1)}$ many solutions $(e_1,\ldots,e_t)$ where $\varepsilon = c-1-(2c-1)/\alpha$ with $p_t = (\log N)^\alpha$. Here we have $\varepsilon > 0$ if and only if $\alpha > (2c-1)/(c-1)$. We associate with the primes $p_1,\ldots,p_t$ a lattice $L \subset \mathbb{R}^{t+1}$ of rank t and we associate with N a point $\mathbf{N} \in \mathbb{R}^{t+1}$. The above problem of diophantine approximation amounts to finding lattice vectors $\mathbf{z}$ that are sufficiently close to $\mathbf{N}$ in the 1–norm. 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.

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 at least $t+2$ integer vectors $(e_1, \dots, e_t) \in \mathbb{Z}^t$ satisfying $|\sum_{i=1}^t e_i \log p_i - \log N| \leq N^{-c} p_t^{o(1)}$ and $\sum_{i=1}^t |e_i \log p_i| \leq$ (2c - 1) $\log N + 2 \log p_t$ where $c > 1$ and $p_1, \dots, p_t$ 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 $v N$ where $v = \prod_{e_j < 0} p_j^{|e_j|}$. We show in Theorem 1 that $|u - vN| \leq p_t^{1+o(1)}$. Hence the residue $u (\bmod N)$ factorizes completely over the primes $p_1, \dots, p_t$ and we obtain a non trivial congruence $\prod_{e_j > 0} p_j^{e_j} = \pm \prod_{j=1}^t p_j^{b_j} (\bmod N)$. Given $t+2$ of these congruences we compute x, y satisfying $x^2 = y^2 (\bmod N)$ and a factor $\gcd(x+y, N)$ of N.

The above diophantine approximation problem can be formulated as a nearly closest lattice vector problem in the 1–norm. In section 3 we associate with N a point $\mathbf{N} \in \mathbb{R}^{t+1}$ and with the primes $p_1, \dots, p_t$ a lattice $L \subset \mathbb{R}^{t+1}$ of rank t. We show in Theorem 2 that every lattice vector that is sufficiently close to $\mathbf{N}$ in the 1–norm yields a desired diophantine approximation of $\log N$.

Lattice vectors sufficiently close to $\mathbf{N}$ exists if the following two properties are nearly independent for random integers u, v with $0 < u < N^c$, $N^{c-1}/2 < v < N^{c-1}$:

- u and v are free of prime factors larger than p_t.
- $|u - vN| = 1$.

Assuming near independence we show in Theorem 5 that there are at least $N^{\varepsilon + o(1)}$ sufficiently close lattice vectors where $\varepsilon > 0$ if $\alpha > (2c-1)/(c-1)$ holds with $p_t = (\log N)^\alpha$. These results reduce the problem of factoring N to the task of finding lattice vectors in L that are close to $\mathbf{N}$ in the 1–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. This approach with non negative coefficients e_i seemed to be impractical and it was never analysed. We introduce negative coefficients e_i into this approximation problem and we set it up as a closest lattice vector problem. We present explicit numbers on the size of the lattice and error bounds needed to make the method work.

We have produced solutions for the diophantine approximation problem using a prime basis of $t = 125$ primes. We reduce the lattice basis by block Korkin–Zolotarev reduction, a concept that has been introduced by Schnorr (1987). Schnorr and Euchner (1991) give improved practical algorithms for block Korkin–Zolotarev reduction. For a basis of 125 primes the diophantine approximation problem can be solved within a few hours on a SPARC 1+ computer. For lattices of very large rank it may be hard to find lattice vectors that are, in the 1–norm, sufficiently close to a given vector. Our experience with the particular problem indicates that it is sufficient to reduce, by a strong reduction algorithm for the square norm, the lattice basis $b_1, \ldots, b_t, \mathbf{N}$ described in section 3. The reduced basis most likely yields at least one solution of the diophantine approximation problem. More solutions can be found by reducing random permutations of this basis.

In order to factor integers N that are 500 bits long the basis should have about 6300 primes. Moreover the input lattice basis contains integers that are 1500 bits long. The reduction of such a basis is certainly a formidable task but it should not be overestimated. There are several reduction techniques that allow to do most of the arithmetic in single precision floating point. We can start the reduction with Seysen's algorithm using single precision arithmetic or we can use the floating point variant of the L^3–algorithm proposed by Schnorr and Euchner (1991). For lattice bases of dimension 6300 our present reduction algorithms may run several months. Their success rate may be far to low. To make the method work for large N we need to improve the lattice L and the present reduction algorithms.

It has been suggested to use algorithms that directly perform the reduction in the 1–norm. Such algorithms have been proposed by Kaib (1991) and Lovász, Scarf (1990). The Lovász, Scarf algorithm works in arbitrary dimensions but seems to be inefficient for our problem, so far it produced no solutions of the diophantine approximation problem. The Kaib algorithm is quite efficient but it is restricted to lattices of dimension 2.

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 any lattice vectors that are sufficiently close to the point $\mathbf{N}$. We show in section 4 that there are $N^{\varepsilon + o(1)}$ lattice vectors that are sufficiently close to $\mathbf{N}$. In section 5 we reduce the problem of computing discrete logarithms to the task of finding a sufficiently close lattice vector in an associated lattice.

2 Factoring integers via smooth numbers.

Notation Let $\mathbb{N}, \mathbb{Q}, \mathbb{R}$ be the sets of natural, rational, and 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)
$\alpha, c \in \mathbb{Q}$ with $\alpha, c > 1$. (The choice for α, c is discussed in section 3)

1. Form the list $p_1, \ldots, p_t$ of the first t primes, $p_t = (\log N)^\alpha$.

2. Generate from vectors in the lattice $L_{\alpha,c}$ 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

$$\sum_{i=1}^{m} c_i(\mathbf{a}_i + \mathbf{b}_i) = \mathbf{0} \pmod 2$$

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

$$y := \prod_{j=0}^{t} p_j^{\sum_{i=1}^{m} c_i b_{i,j}} \pmod N = \prod_{j=0}^{t} p_j^{\sum_{i=1}^{m} c_i a_{i,j}} \pmod N .$$

   (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 the integers 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 at least $t+2$ pairs (u_i, v_i) needed 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 the lattice $L_{\alpha,c}$ and we show that every vector in $L_{\alpha,c}$ that is sufficiently close to the point $\mathbf{N}$ yields some pair $(u_i, v_i) \in \mathbb{N}^2$ 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 in the 1–norm.

Let $\alpha, c > 1$ be fixed and let $p_1, \ldots, p_t$ be the first t primes, $p_t = (\log N)^\alpha$. 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 the following column vector:

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

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 *1–norm* of a vector $\mathbf{z} = (z_1, \ldots, z_{t+1}) \in \mathbb{R}^{t+1}$ is by definition $\|\mathbf{z}\|_1 = \sum_{i=1}^{t+1} |z_i|$. All asymptotic assertions are for $N \to \infty$, e.g. $\lim_{N\to\infty} o(1) = 0$.

Theorem 1. *Let $c > 1$, β, $\delta \geq 0$ be fixed and let $p_t < N$. If $(e_1, \dots, e_t) \in \mathbb{Z}^t$ satisfies the inequalities*

$$\Big| \sum_{i=1}^{t} e_i \log p_i - \log N \Big| \;\leq\; N^{-c} p_t^{\beta + o(1)} \tag{3}$$

$$\sum_{i=1}^{t} |e_i \log p_i| \;\leq\; (2c-1)\log N + 2\delta \log p_t \tag{4}$$

then we have for $u := \prod_{e_j<0} p_j^{e_j}$, $v := \prod_{e_j<0} p_j^{|e_j|}$ that $|u - vN| \leq p_t^{\beta+\delta+o(1)}$.

We see that if $(e_1, \dots, e_t)$ satisfies the inequalities 3 and 4 with $\beta + \delta \leq 1$ and N is sufficiently large then the pair (u, v) most likely has the properties 1 and 2 desired for the factoring algorithm. Since $|u - vN|$ may be slightly larger than p_t there is a small chance that $|u - vN|$ does not factor completely over the primes $p_1, \cdots, p_t$. Theorem 4 suggests that this chance is negligible. The factoring method also works for fixed $\beta + \delta > 1$. There is a chance of about $(\beta + \delta)^{-\beta-\delta}$ that $|u - vN|$ factors completely over the primes $p_1, \dots, p_t$.

Proof. We see from Inequality 3 that

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

Using that $\log(1 + x) = x + O(x^2)$ holds for $|x| \leq 1/2$ this yields

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

It remains to prove that $v \leq N^{c-1} p_t^{\delta+o(1)}$. We have

$$\begin{aligned} \log v \;&\overset{(3)}{\leq}\; \log u - \log N + N^{-c} p_t^{o(1)} \\ &\overset{(4)}{\leq}\; -\log v + (2c - 1 - 1)\log N + 2\delta \log p_t + N^{-c} p_t^{\beta+o(1)}. \end{aligned}$$

Hence $2\log v \leq 2(c-1)\log N + 2\delta \log p_t + N^{-c} p_t^{o(1)}$ and thus $v \leq N^{c-1} p_t^{\delta}(1 + o(1))$. **QED**

Theorem 2. *Let $\alpha, c > 1, \delta > 0$ be fixed and $(\log N)^{\alpha} = p_t < N$. If $\mathbf{z} \in L$ satisfies the inequality*

$$\|\mathbf{z} - \mathbf{N}\|_1 \;\leq\; (2c-1)\log N + 2\delta \log p_t \tag{5}$$

then we have for $(u, v) := g(\mathbf{z})$ that $|u - vN| \leq p_t^{1/\alpha+\delta+o(1)}$.

The lattice vectors $\mathbf{z}$ constructed in our experiments usually have smaller values $|u - vN|$ than those predicted by the upper bound $p_t^{1/\alpha+\delta+o(1)}$. For $\alpha = 2$ we always found values $|u - vN| < p_t^{\delta}$.

Proof. Let $\mathbf{z} = \sum_{i=1}^{t} e_i \mathbf{b}_i$. We show that the inequality 5 implies the inequalities 3 and 4 with $\beta = 1/\alpha$. Then the claim follows from Theorem 1.
" $5 \Rightarrow 3$ ". It follows from Inequality 5 that

$$|(\mathbf{z} - \mathbf{N})_{t+1}| \ \leq \ (2c-1)\log N + 2\delta \log p_t \ = \ p_t^{1/\alpha+o(1)} \ .$$

Since $|(\mathbf{z} - \mathbf{N})_{t+1}| = N^c |\sum_{i=1}^{t} e_i \log p_i - \log N|$ this proves Inequality 3 with $\beta = 1/\alpha$.
" $5 \Rightarrow 4$ ". Inequality 5 implies Inequality 4 since

$$\sum_{i=1}^{t} e_i \log p_i \ \leq \ \|\mathbf{z} - \mathbf{N}\|_1.$$

QED

Thus in order to factorize N it is sufficient to produce lattice points $\mathbf{z}$ that are close to $\mathbf{N}$ in the 1–norm. Such lattice points can be found in practice by reducing the basis $\mathbf{b}_1, \ldots, \mathbf{b}_t, \mathbf{N}$ using a strong reduction algorithm for the square norm. The reduced basis usually contains at least some vector $\mathbf{b}$ that is very short in the 1–norm. With some care we can achieve that this vector is of the form $\mathbf{b} = \sum_{i=1}^{t} e_i \mathbf{b}_i - \mathbf{N}$. This solves Inequality 5 with $\mathbf{z} = \sum_{i=1}^{t} e_i \mathbf{b}_i$.

Rational approximation of the basis matrix. In practice we must approximate the real vectors $\mathbf{b}_1, \ldots, \mathbf{b}_t, \mathbf{N}$ by rational vectors. The approximation must be sufficiently close so that the error for $\mathbf{z} = \sum_{i=1}^{t} e_i \ \mathbf{b}_i$ is negligible whenever Inequality 5 holds. In practice 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 Inequality 5 of Theorem 2 where $\varepsilon = c - 1 - (2c-1)/\alpha$ with $p_t = (\log N)^{\alpha}$. Our argument showing the existence of these lattice vectors $\mathbf{z} \in L$ is not constructive. We generate these lattice vectors from smooth integers u, v satisfying $|u - vN| = 1$. The existence of these smooth integers follows from the assumption that the smooth integers u and v distribute almost independently from the inequality $|u - vN| = 1$.

Let $\mathbb{N}_t$ denote the set of integers that factorize completely over the primes $p_1, \ldots, p_t$. The integers in $\mathbb{N}_t$ are called *p_t–smooth.* 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, 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 3. *If* $u, v \in \mathbb{N}_t$, $|u - vN| = o(N^c)$ *and* $v = \Theta(N^{c-1})$ *then* $\mathbf{z} = f(u,v)$ *satisfies* $\|\mathbf{z} - \mathbf{N}\|_1 \leq (2c-1)\log N + O(|u - vN|)$.

Proof. We have

$$\|\mathbf{z} - \mathbf{N}\|_1 \;=\; \log u + \log v + N^c \; |\log \frac{u}{vN}|.$$

We see from $v = \Theta(N^{c-1})$, $|u - vN| = o(N^c)$ that

$$\log u + \log v \;=\; (2c-1)\log N + O(1).$$

Moreover

$$|\log \frac{u}{vN}| \;=\; |\log\left(1 + \frac{u - vN}{vN}\right)| \;=\; O\left(\frac{|u - vN|}{N^c}\right).$$

This proves the claim. **QED**

In order to estimate the number of small pairs $(u,v) \in \mathbb{N}_t^2$ with $|u - vN| = 1$ we will assume the following

Hypothesis. *For fixed* $\alpha, c > 1$ *and for* $N \to \infty$ *the fraction of pairs* (u,v) *in* $\{(u,v) \in \mathbb{N}^2 \,|\, N^{c-1}/2 < v < N^{c-1}, |u - vN| = 1\}$ *for which u and v are* $(\log N)^\alpha$*–smooth is at least* $1/(\log N)^{O(1)}$*–times the probability that a random pair in*

$$\{(u,v) \in \mathbb{N}^2 \,|\, u \leq N^c,\; N^{c-1}/2 < v < N^{c-1}\}$$

is $(\log N)^\alpha$*–smooth in u and v.*

The hypothesis means that for random integers u, v of order N^c and N^{c-1} the following events are nearly independent for large N

- both u and v are $(\log N)^\alpha$–smooth
- $|u - vN| = 1$.

We can replace the equality $|u - vN| = 1$ by the inequality $|u - vN| \le \log p_t$ and we can work with this inequality instead. By Lemma 3 any p_t–smooth integers u, v satisfying this inequality yield a lattice vector $\mathbf{z} = f(u, v)$ such that

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

Conversely by Theorem 2, every lattice vector $\mathbf{z}$ with the latter property yields a pair of p_t–smooth integers u and v such that $|u - vN| = p_t^{O(1)}$.

The following theorem is at the base of various factoring algorithms.

Theorem 4. (NORTON 1971 and CANFIELD, ERDÖS, POMERANCE, 1983) *Let* $\varepsilon > 0$ *be fixed and let* r *satisfy* $N^{1/r} \ge (\log N)^{1+\varepsilon}$. *Then* $\#\{x \le N \,|\, x$ *is free of primes* $> N^{1/r}\} \,/\, N = r^{-r+o(r)}$ *where* $\lim\limits_{N\to\infty} o(r)/r = 0$.

Let

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

Theorem 5. *Suppose the hypothesis holds. Then for fixed* $\alpha, c > 1$ *and for* $N \to \infty$ *there are at least* $N^{\varepsilon + o(1)}$ *many vectors* $\mathbf{z} \in L$ *that satisfy Inequality 5 where* $\varepsilon = (c-1) - (2c-1)/\alpha$.

I.e. if $\alpha > (2c-1)/(c-1)$ then there are exponentially many lattice vectors that satisfy Inequality 5.

Proof. Let $r = \log N \,/\, \alpha \log\log N$, and thus $(\log N)^{\alpha} = N^{1/r}$. By the hypothesis and Theorem 4 we have for sufficiently large N that

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

This yields

$$\begin{array}{lcl} \log \# M_{\alpha,c,N} & \ge & (c-1)\log N - \frac{\log N}{\alpha \log\log N}\left((c-1)\log[r(c-1)] + c\log cr\right) \\ & & + o(r \log cr) \\ & \overset{cr \le \log N}{\ge} & [(c-1) - (2c-1)\alpha^{-1}]\log N + o(\log N) \\ & = & (\varepsilon + o(1))\log N \quad \text{with} \quad \varepsilon = (c-1) - (2c-1)\alpha^{-1}. \end{array}$$

Hence $\# M_{\alpha,c,N} \ge N^{\varepsilon + o(1)}$. Since the integers u, vN with $|u - vN| = 1$ are coprime the function f is one–one on $M_{\alpha,c,N}$. Hence $\# f(M_{\alpha,c,N}) = N^{\varepsilon+o(1)}$. By Lemma 3 we have for all $(u,v) \in M_{\alpha,c,N}$ that $\mathbf{z} = f(u,v)$ satisfies Inequality 5. This proves the claim. **QED**

Conclusion. We have reduced, by the algorithm in section 2, Theorem 1 and Theorem 5, the problem of factoring N to the problem of finding $t+2$ solutions $(e_1, \ldots, e_t)$ of the inequalities 3 and 4 (to the problem of finding $t+2$ lattice vectors $\mathbf{z}$ satisfying (5), resp.). Our reduction is polynomial time. Its correctness uses two heuristic arguments. First, we assume that $x \neq \pm y \pmod{N}$ holds with positive probability for the solution of the congruence $x^2 = y^2 \pmod{N}$ generated by the algorithm. Second, we assume in the hypothesis that the smooth integers u, v distribute independently from the equality $|u - vN| = 1$.

The condition $\alpha > (2c-1)/(c-1)$ in Theorem 5 can be relaxed for small N. We give examples of parameters α, c so that $\#M_{\alpha,c,N}$ is larger than t.

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

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

The corresponding lattice problem is unfeasible for the presently known lattice reduction algorithms. 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.

Example solutions of the inequalities 3 and 4 using a basis of 125 primes.
Using $t = 125$ primes with the largest prime $p_t = 691$ we have solved the inequalities 3 and 4 (1 and 2, resp.) for $N = 2131438662079$, $N^c = 10^{25}$, $c \approx 2.0278$ and $\alpha \approx 1.954$. Simple L^3–reduction did not generate any solution of the inequalities 3 and 4 for this N. We have reduced the lattice basis B of section 3 with 4 precision bits to the right of the point using block Korkin–Zolotarev reduction with block size 32. The general concept of block Korkin–Zolotarev reduction has been developped in Schnorr (1987). Schnorr and Euchner (1991) give practical algorithms and evaluate their performance in solving subset sum problems. Finding a single solution took a couple of hours on a SPARC 1+ computer.

Example solutions

1. $u = 2^2 \cdot 3^9 \cdot 7^5 \cdot 19 \cdot 41 \cdot 59 \cdot 61 \cdot 97 \cdot 181 \cdot 211 \cdot 223$
   $v = 37 \cdot 43 \cdot 73 \cdot 151 \cdot 163 \cdot 503$, $u - vN = 1$
   The vector $\mathbf{z} = f(u, v)$ satisfies $\|\mathbf{z} - \mathbf{N}\|_1 \approx 88.43 \approx (2c-1)\log N + 1.69$.

2. $u = 3^4 \cdot 5^3 \cdot 11^2 \cdot 17 \cdot 19 \cdot 61 \cdot 67 \cdot 73 \cdot 109 \cdot 193 \cdot 211 \cdot 233 \cdot 263$
   $v = 2 \cdot 59 \cdot 101 \cdot 127 \cdot 163 \cdot 173 \cdot 353,\ u - vN = 7.$
   The vector $\mathbf{z}$ satisfies $\|\mathbf{z} - \mathbf{N}\|_1 \approx 91.02 \approx (2c-1)\log N + 4.28.$

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

4. $u = 3^2 \cdot 5^4 \cdot 17 \cdot 19 \cdot 67 \cdot 71 \cdot 137 \cdot 173 \cdot 191 \cdot 211 \cdot 509 \cdot 593$
   $v = 2^2 \cdot 7 \cdot 13 \cdot 31 \cdot 43 \cdot 47 \cdot 97 \cdot 157 \cdot 239\ ,\ u - vN = 89.$
   The vector $\mathbf{z}$ satisfies $\|\mathbf{z} - \mathbf{N}\|_1 \approx 96.98 \approx (2c-1)\log N + 10.23.$

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 $\|\mathbf{z} - \mathbf{N}\|_1 \approx 97 \approx (2c-1)\log N + 10.26.$

6. $u = 3 \cdot 19 \cdot 47 \cdot 67 \cdot 71 \cdot 97 \cdot 113 \cdot 151 \cdot 157 \cdot 199 \cdot 239 \cdot 269 \cdot 359$
   $v = 17 \cdot 31 \cdot 107 \cdot 137 \cdot 211 \cdot 223 \cdot 373,\ u - vN = 166.$
   The vector $\mathbf{z}$ satisfies $\|\mathbf{z} - \mathbf{N}\|_1 \approx 98.58 \approx (2c-1)\log N + 11.84.$

Remarks on the experiment. The inequality $\|\mathbf{z} - \mathbf{N}\|_1 \le (2c-1)\log N + 2\delta \log p_t$ with $2 \log p_t \approx 13.07$ was always sufficient to generate p_t–smooth integers u and v satisfying $|u - vN| < p_t^\delta$. Thus $|u - vN|$ is in practice smaller than the upper bound $p_t^{1/\alpha+\delta+o((1)}$ of Theorem 2.
2. The parameter $\alpha \approx 1.954$ was considerably smaller than the value $(2c-1)/(c-1) \approx 2.9752$ of Theorem 5. Thus there may be sufficiently many close lattice vectors even if α is smaller than $(2c-1)/(c-1)$.
3. Under the hypothesis we have with $r = \log N/\alpha \log\log N \approx 28.39$ that

$$\begin{aligned} \log \# M_{\alpha,c,N} &\lesssim (c-1)\log N - r(c-1)\log r(c-1) - rc\log rc \\ &\approx 3.35 \end{aligned}$$

5 Computing discrete logarithms.

We reduce the problem of computing discrete logarithms in $\mathbb{Z}_N^*$ to the problem of finding a nearly closest lattice vector in the 1–norm.

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 $m \geq t+2$ general congruences of the form

$$\prod_{j=1}^{t} p_j^{a_{i,j}} \; z^{a_{i,t+1}} \; y^{a_{i,t+2}} \;=\; \prod_{j=0}^{t} p_j^{b_{i,j}} (\operatorname{mod} N) \text{ for } i = 1 \ldots m \tag{6}$$

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

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

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 (6) can be obtained from vectors in the following lattice $L = L_{\alpha,c,z,y} \subset \mathbb{R}^{t+3}$ that are close to the vector $\mathbf{N}$ in the 1–norm. 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.

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

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 $u (\operatorname{mod} N)$ factorizes completely over the basis $p_0 = -1, p_1, \ldots, p_t$ this yields a congruence of the form 6.

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

References

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

2. M.J. Coster, A. Joux, B.A. LaMacchia, A.M. Odlyzko, C.P. Schnorr and J. Stern: *An Improved low–density subset sum algorithm.* Computational complexity 2, (1992), pp. 111 – 128.

3. M. Kaib: *The Gauß lattice basis reduction algorithm succeeds in any norm.* Proceedings of FCT–symposium 1991, Ed. L. Budach, Lecture Notes in Computer Science, 529 (1991), pp. 275 – 286.

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

5. J.C. Lagarias, H.W. Lenstra, Jr. and C.P. Schnorr: *Korkin–Zolotarev bases and successive minima of a lattice and its reciprocal lattice.* Combinatorica, 10 (1990), pp. 333 – 348.

6. A.K. Lenstra, H.W. Lenstra, Jr. and L. Lovász: *Factoring polynomials with rational coefficients.* Math. Annalen 261, (1982), pp. 515–534.

7. L. Lovász: *An algorithmic theory of numbers, graphs and convexity.* SIAM Publications, Philadelphia (1986).

8. L. Lovász and H.E. Scarf: *The generalized basis reduction algorithm.* Math. Oper. Research, 17 (1992), pp. 751 – 764.

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

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

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

12. C.P. Schnorr and M. Euchner: *Lattice basis reduction: improved practical algorithms and solving subset sum problems.* Proceedings of FCT–symposium 1991, Ed. L. Budach, Lecture Notes in Computer Science, 529 (1991), pp. 68–85.