Factoring Integers by CVP and SVP Algorithms

Claus Peter Schnorr

Fachbereich Informatik und Mathematik, Goethe-Universität Frankfurt, PSF 111932, D-60054 Frankfurt am Main, Germany.
schnorr@cs.uni-frankfurt.de

work in progress 21.02.2020

Abstract. To factor an integer $N$ we construct about $n$ triples of $p_n$-smooth integers $u,v,|u-vN|$ for the $n$-th prime $p_n$. We find these triples from nearly shortest vectors of the lattice $L_{n,c}$ whose basis $[B_{n,c},N_c]$ consists of the prime number lattice of the first $n$ primes and a target vector $N_c = (0,...,0,N \cdot \ln N)^t \in \mathbb{R}^{n+1}$ representing $N$. We factor $N \approx 10^{14}$ in 30 seconds by an SVP algorithm for the lattice $L_{n,c}, n=90$. We extend these algorithms to $N \approx 2^{800}$ and $N \approx 2^{800}$ by primal-dual reduction and use lattices of $n=191$ and 383. These new algorithms find short vectors much faster than previous algorithms of KANNAN [Ka87] and FINCKE, POHST [FP85] that disregard the success rate of stages. This greatly reduces the number of stages for finding a shortest/closest lattice vector.

Keywords. Prime number lattice, Primal-dual reduction.

1 Introduction and survey

The enumeration algorithm ENUM of [SE94, SH95] for short lattice vectors cuts stages by linear pruning. For NEW ENUM we introduce the success rate $\beta_i$ of stages based on the GAUSSIAN volume heuristic. NEW ENUM first performs stages with high success rate and stores stages of smaller but still reasonable success rate for later performance. NEW ENUM finds short vectors much faster than previous algorithms of KANNAN [Ka87] and FINCKE, POHST [FP85] that disregard the success rate of stages.

Section 4 presents time bounds of ENUM under linear pruning for SVP for a lattice basis $B = [b_1,...,b_n] \in \mathbb{Z}^{n \times n}$. Prop. 1 shows that ENUM finds under linear pruning a shortest lattice vector $b$ that behaves randomly (SA) under the volume heuristics in polynomial time if $B$ satisfies GSA and $rd(L) = o(n^{-1/4})$ holds for the relative density $rd(L)$ of lattice $L$, see section 2. It follows that the maximal SVP-time of ENUM under linear pruning for lattices of dim. $n$ is $n^{\frac{3}{2} + \big(1+o(1))}$. Cor. 3 translates Prop. 1 from SVP to CVP proving pol. time under similar conditions as Prop. 1 if $\|L - t\| \leq \lambda_1$ holds for the target vector $t$.

Sections 5, 6 study factoring algorithms first for $N \approx 10^{14}$ and then for $N \approx 2^{400}$ and $N \approx 2^{800}$ based on reduction algorithms for the lattice $L_{n,c}$ with basis matrix $[B_{n,c},N_c]$. The programs for factoring $N \approx 10^{14}$ are from master thesis of M.Charlet and A.Schickedanz and construct $p_n$-smooth integers $u,v,|u-vN|$ by an SVP-algorithm for $L_{n,c}$. For $N \approx 2^{400}$ and $N \approx 2^{800}$ we primal-dual reduce of the basis $[B_{n,c},N_c]$ using blocks of dimension 24. To factor $N \approx 2^{800}$ we construct a vector $b \in L(B_{n,c}), b \sim (u,v)$ with $p_n$-smooth $u,v$ and $v \leq p_n$ such that $|u-vN|$ is $p_n$-smooth with probability 0.128. We easily obtain from this $(u,v)$ enough fac-relations to factor $N$. Integers $N \approx 2^{400}$ and $N \approx 2^{800}$ are factored by $3.34 \cdot 10^{13}$ and $6 \cdot 10^{13}$ arithmetic operations, much faster and using a much smaller prime basis than the quadratic sieve QS and the number field sieve NFS.

2 Lattices

Let $B = [b_1,...,b_n] \in \mathbb{R}^{m \times n}$ be a basis matrix consisting of $n$ linearly independent column vectors $b_1,...,b_n \in \mathbb{R}^m$. They generate the lattice $L(B) = \{Bx | x \in \mathbb{Z}^n\}$ consisting of all integer linear combinations of $b_1,...,b_n$. The dimension of $L$ is $n$, the determinant of $L$ is $\det L = (\det B'B)^{1/2}$ for any basis matrix $B$ and the transpose $B'$ of $B$. The length of $b \in \mathbb{R}^m$ is $\|b\| = (b'b)^{1/2}$.
Let $\lambda_1 = \lambda_1(L)$ be the length of the shortest nonzero vector of $L$. The Hermite constant $\gamma_n$ is the minimal $\gamma$ such that $\lambda_1^2 \leq \gamma^n$ holds for all lattices of dimension $n$.

The basis matrix $B$ has the unique QR factorisation $B = QR \in \mathbb{R}^{n \times n}$, $R = [r_{ij}]_{1 \leq i,j \leq n} \in \mathbb{R}^{n \times n}$ where $Q \in \mathbb{R}^{n \times n}$ is isometric (with pairwise orthogonal column vectors of length 1) and $R \in \mathbb{R}^{n \times n}$ is upper-triangular with positive diagonal entries $r_{ii}$. The QR-factorization provides the Gram-Schmidt coefficients $\mu_{ij} = r_{ij}/r_{ii}$, which are rational for integer matrices $B$. The orthogonal projection $B^\ast$ of $b_1$ in $\text{span}(b_1, \ldots, b_{i-1})^\perp$ has length $r_{ii} = \|b_i\| = \|b_i^\ast\| = |r_{1i}|$.

LLL-bases. A basis $B = QR$ isLLL-reduced or an LLL-basis for $\delta \in (\frac{1}{2}, 1)$ if

1. $|r_{ij}|/r_{ii} \leq \frac{1}{2}$ for all $j > i$.
2. $\delta r_{ii}^2 \leq r_{i+1,i+1}^2 + r_{i+1,i+1}^2$ for $i = 1, \ldots, n-1$.

Obviously, LLL-bases satisfy $\delta r_{ii}^2 \leq \alpha r_{i+1,i+1}^2$ for $\alpha := 1/(\delta - \frac{1}{4})$. [LLL82] introduced LLL-bases focusing on $\delta = 3/4$ and $\alpha = 2$. A famous result of [LLL82] shows that LLL-bases for $\delta < 1$ can be computed in polynomial time and that they nicely approximate the successive minima:

3. $\alpha^{-i+1} \leq \|b_i\|^2 \lambda_i^{-2} \leq \alpha^{n-1}$ for $i = 1, \ldots, n$.

4. $\|b_i\|^2 \leq \alpha^{\frac{n-1}{2}} (\det L)^{\frac{n}{2}}$.

A basis $B = QR \in \mathbb{R}^{n \times n}$ is an HKZ-basis (Hermite, Korkine, Zolotareff) if $|r_{ij}|/r_{ii} \leq \frac{1}{2}$ for all $j > i$, and if each diagonal entry $r_{ii}$ of $R = [r_{ij}] \in R^{n \times n}$ is minimal under all transforms of $B$ to $BT$, $T \in \text{GL_n}(\mathbb{Z})$ that preserve $B_1, \ldots, B_{i-1}$.

A basis $B = QR \in \mathbb{R}^{n \times n}$, $R = [r_{ij}]_{1 \leq i, j \leq n}$ is a BKZ-basis for block size $k$, i.e., a BKZ-$k$ basis if the matrices $[r_{ij}]_{1 \leq i, j \leq k}$ form HKZ-bases for $h = 1, \ldots, n-k+1$, see [SE94].

The shortest vector problem (SVP): Given a basis of $L$ find a shortest nonzero vector of $L$, i.e., a vector of length $\lambda_1$. The closest vector problem (CVP): Given a basis of $L$ and a target $t \in \text{span}(L)$ find a closest vector $b' \in L$ such that $\|t - b'\| = \|t - L\| = \min \{\|t - b\| : b \in L\}$.

The efficiency of our algorithms depends on the lattice invariant $rd(L) := \lambda_1 \gamma_n^{-1/2} (\det L)^{-1/n}$, thus $\lambda_1^2 = rd(L)^2 \gamma_n (\det L)^{\frac{1}{n}}$ which we call the relative density of $L$. Clearly $0 < rd(L) \leq 1$ holds for all $L$, and $rd(L) = 1$ if and only if $L$ has maximal density. Lattices of maximal density and $\gamma_n$ are known for $n = 1, \ldots, 8$ and $n = 24$.

3 Efficient enumeration of short lattice vectors

We outline the SVP-algorithm based on the success rate of stages. New Enum improves the algorithm Enum of [SE94, SH95]. We recall Enum and present New Enum as a modification that essentially performs all stages of Enum in decreasing order of success rates. This SVP-algorithm New Enum finds a shortest lattice vector fast without enumerating all short lattice vectors.

Let $B = [b_1, \ldots, b_n] = QR \in \mathbb{R}^{n \times n}, R = [r_{ij}]_{1 \leq i, j \leq n} \in \mathbb{R}^{n \times n}$, be the given basis of $L = L(B)$. Let $\pi : \text{span}(b_1, \ldots, b_n) \to \text{span}(b_1, \ldots, b_{i-1})^\perp = \text{span}(b^\ast_1, \ldots, b^\ast_n)$ for $i = 1, \ldots, n$ denote the orthogonal projections and let $L_i = L(b_1, \ldots, b_{i-1})$.

The success rate of stages. At stage $u = (u_1, \ldots, u_n)$ of Enum for SVP of $L$ a vector $b = \sum_{i=1}^n u_i b_i \in L$ is given such that $\|\pi_i(b)\|^2 \leq \lambda_i^\ast$. (When $\lambda_i^\ast$ is unknown we use instead some $\lambda_i > \lambda_i^\ast$.) Stage $u$ calls the substages $(u_{i-1}, \ldots, u_n)$ such that $\|\pi_{i-1}(\sum_{i=1}^n u_i b_i)\|^2 \leq \lambda_i^\ast$. We have $\|\sum_{i=1}^n u_i b_i\|^2 = \sum_{i=1}^n u_i b_i \|^2 + \|\pi_1(b)\|^2$, where $\zeta_i := b - \pi_i(b) \in \text{span} L_i$ is $b$'s orthogonal projection in span $L_i$. Stage $u$ and its substages enumerate the intersection $B_{i-1} \cap L_i$ of the sphere $B_{i-1} \subset \text{span} L_i$ with radius $\sqrt{\zeta_i} := (\lambda_i^2 - \|\pi_1(b)\|^2)^{1/2}$ and center $\zeta_i$. The GAUSSIAN volume heuristics estimates for $t = 1, \ldots, n$ the expected size $|B_{i-1} \cap (L_i + \zeta_i)|$ to be the success rate

$$\beta_i(u) = \frac{\text{vol} B_{i-1}(0, \zeta_i)}{\text{det} L_i} \quad (3.1)$$

standing for the probability that there is an extension $(u_1, \ldots, u_n)$ of $u = (u_1, \ldots, u_n)$ such that $|\sum_{i=1}^n u_i b_i| \leq \lambda_i$. Here $\text{vol} B_{i-1}(0, \zeta_i) = (1/2)^{n-1} V_{n-1} \zeta_i^{n-1}$. $V_{n-1} = \pi^n / (2^n n!)$ is the volume of the unit sphere of dimension $n-1$ and $\text{det} L_i = r_{1i} \cdots r_{n-1,i}$. If $\zeta_i \in \text{span} L_i$ is uniformly distributed the expected size of this intersection satisfies $E_{\zeta_i} [\#(B_{i-1} \cap (L_i + \zeta_i))] = \beta_i(u)$. This holds because $1/\text{det} L_i$ is the number of lattice points of $L_i$ per volume in span $L_i$. We do not simply cut $u_i$ due to a small $\beta_i$ because there might be a vector in $L_i$ very close to $\zeta_i$. 2
The success rate $\beta_t$ has been used in [SH95] to speed up ENUM by cutting stages of very small success rate. New ENUM first performs all stages with sufficiently large $\beta_t$ giving priority to small $t$ and collects during this process the unperformed stages in the list $L$. For instance it first performs all stages with $\beta_t \geq 2^{-\varepsilon} \log t$, where $\varepsilon = \log_2 3$. Thereafter New ENUM increases $s$ to $s + 1$. So far our experiments simply perform all stages with $\beta_t \geq 2^{-\varepsilon}$. If $\lambda_2^t$ is unknown we can compute $\rho_t$, $\beta_t$ replacing $\lambda_2^t$ by the upper bound $A = \frac{1.744}{e^2}n \det(B'B)^{\frac{1}{2}} \geq \lambda_2^t$ which holds since $\gamma_n \leq \frac{1.744}{e^2}n \approx 0.10211 n$ holds for $n \geq n_0$ by a computer proof of Kabatiansky, Levenstein [KaLe78].

Dabei ist $e = 2.7182818284 \ldots$ die Eulersche Zahl und $\pi = 3.141592654 \ldots$ die Kreiszahl.

Outline of New ENUM

**INPUT** BKZ-basis $B = QR$, $R = [r_{i,j}] \in \mathbb{R}^{n \times n}$ of block size $32$, $A$, $s = \log n = \log_2 n$

**OUTPUT** a sequence of $b \in L(B)$ of decreasing length terminating with $\|b\| = \lambda_1$.

1. $L := \emptyset$.
2. Let New Enum perform all stages $u_t = (u_t, \ldots, u_{n})$ with $\beta_t(u) \geq 2^{-\varepsilon} \log t$.
   
   Upon entry of stage $(u_t, \ldots, u_{n})$ compute $\beta_t(u_t)$. If $\beta_t(u_t) < 2^{-\varepsilon} \log t$ then store $(u_t, \ldots, u_{n})$ in the list $L$ of delayed stages. Otherwise perform stage $(u_t, \ldots, u_{n})$, let $t := t - 1$, $u_t := [-\sum_{t+1}^n u_{t+1} / r_{t,t}]$ and go to stage $(u_t, \ldots, u_{n})$. If for $t = 1$ some $b \in L \setminus 0$ of length $\|b\|^2 \leq A$ has been found,
   
   give out $b$, we can then decrease $A := \|b\|^2 - 1$ if $R^TR \in \mathbb{Z}^{n \times n}$.
3. $s := s + 1$. IF $L \neq \emptyset$ THEN perform all stages $u_t \in L$ with $\beta_t(u_t) \geq 2^{-\varepsilon} \log t$.

**Running in linear space.** If instead of storing the list $L$ we restart New ENUM in step 3 on level $s + 1$ then New ENUM runs in linear space and its running time increases at most by a factor $n$.

**Practical optimization.** New ENUM computes $R_t, \beta_t, V_t, \rho_t, c_t$ in floating point and $b_t, \|b_t\|^2$ in exact arithmetic. The final output $b$ has length $\|b\| = \lambda_1$, but this is only known when the more expensive final search does not find a vector shorter than the final $b$.

**Reason of efficiency.** For short vectors $b = \sum_{t=1}^n u_t b_t \in L \setminus 0$ the stages $u_t = (u_t, \ldots, u_{n})$ have large success rate $\beta_t(u)$. On average $\|\pi_t(b)\|^2 \approx \frac{n^{-\varepsilon}}{\lambda_2^t}$ holds for a random $b \in R B_t(0, \lambda_1)$ of length $\lambda_1$. Therefore $g_t^2 = A - \|\pi_t(b)\|^2$ and $\beta_t(u)$ are large. New ENUM tends to output very short lattice vectors first.

New ENUM is particularly fast for small $\lambda_1$. The size of its search space approximates $\lambda_1^t V_n$, and is by Prop. 1 heuristically polynomial if $rd(L) = o (n^{-1/4})$. Having found $b'$ New ENUM proves $\|b'\|^2 = \lambda_1$ in exponential time by a complete exhaustive enumeration.

**Notation.** We use the following function $c_t : \mathbb{Z}^{n-t+1} \to \mathbb{R}$:

$$c_t(u_1, \ldots, u_{n}) = \|\pi_t(\sum_{t=1}^n u_t b_t)\|^2 = \sum_{t=1}^n (\sum_{j=1}^n u_j r_{j,t})^2.$$

Hence

$$c_t(u_1, \ldots, u_{n}) = \left(\sum_{t=1}^n u_t r_{t,t}\right)^2 + c_{t+1}(u_{t+1}, \ldots, u_{n}).$$

Given $u_{t+1}, \ldots, u_{n}$ Enum takes for $u_t$ the integers that minimize $|u_t + y_t|$ for $y_t := \sum_{t+1}^n u_{t+1} r_{t,t}$ in order of increasing distance to $-y_t$ adding to the initial $u_t := -[y_t]$ iteratively $[\nu_t/2](-1)^{c_t}$ where $c_t := sign(u_t + y_t) \in \{\pm 1\}$ and $\nu_t$ numbers the iterations starting with $\nu_t = 0, 1, 2, \ldots$ :

$$-|y_t|, -|y_t| - c_t, -|y_t| + c_t, -|y_t| + 2c_t, -|y_t| + 2c_t, \ldots, -|y_t| + \lceil \nu_t/2 \rceil (-1)^c_t \ldots,$$

where $sign(0) := 1$ and $[r]$ denotes a nearest integer to $r \in \mathbb{R}$. The iteration does not decrease $|u_t + y_t|$ and $c_t(u_1, \ldots, u_{n})$, it does not increase $\rho_t$ and $\beta_t$. Enum performs the stages $(u_t, \ldots, u_{n})$ for fixed $u_{t+1}, \ldots, u_{n}$ in order of increasing $c_t(u_1, \ldots, u_{n})$ and decreasing success rate $\beta_t$. $\beta_t$ extends this priority to stages of distinct $t, t'$ taking into account the size of two spheres of distinct dimensions $n - t, n - t'$: The center $C_t = b - \pi_t(b) = \sum_{t=1}^n u_t (b_t - \pi_t(b_t)) \in \text{span}(L_t)$ changes continuously within New Enum which improves Enum from [SH95].
New Enum for SVP

INPUT B = QR, R = \([r_{i,j}]\) ∈ \(\mathbb{R}^{n \times n}\), A ≥ \(\lambda^2\), \(s_{max}\)

OUTPUT a sequence of points \(b \in \mathcal{L}(B)\) such that \(||b||\) decreases to \(\lambda_1\).

1. \(L := \emptyset\), \(t := t_{max} := 1\), FOR \(i = 1, \ldots, n\) DO \(c_i := u_i := y_i := 0\), \(\nu_i := u_i := 1\), \(s := 5\), \(c_1 := r_{1,1}\), \(c_i = c_i(u_i, \ldots, u_n)\) always holds for the current \(t\).

2. WHILE \(t ≤ n\) \#perform stage \(u_i := (u_i, \ldots, u_n, y_i, c_i, \nu_i, \sigma_i, \beta_i, A)\):
   \(c_i := c_i + (u_i + y_i)^2 r_{i,1}^2\), \(\beta_i := (A - c_i)^{1/2}\), \(\nu_i := \min \left(\frac{|y_i|}{r_{i,1}}, \frac{1}{\nu_i} \right)\).
   IF \(c_i ≥ A\) THEN \(t := t + 1\), \(t_{max} := \max (t, t_{max})\).
   IF \(||b||^2 < A\) THEN \(\nu_i := \min (\nu_i, 1)\).
   \(t := t + 1\), \(t_{max} := \max (t, t_{max})\).
   ELSE \(\beta_i ≥ 2^{s_{max}}\) THEN \(\nu_i := \nu_i \min (\nu_i, 1)\).
   \(t := t + 1\), \(t_{max} := \max (t, t_{max})\).
   \(t := t_{max}\).
   \(\nu_i := 1\), \(\nu_i := 0\).

3. perform all stages \(u_i := (u_i, \ldots, u_n, y_i, c_i, \nu_i, \sigma_i, \beta_i, A) \in L\) with \(\beta_i ≥ 2^{-s}\).

4. \(s := s + 1\), IF \(s > s_{max}\) THEN restart with a larger \(s_{max}\).

When step 3 performs stages \(u_i \in L\) the current \(A\) can be smaller than the \(A\) of \(u_i\) and this can make the stored \(\beta_i\) of \(u_i\) smaller than \(2^{−s}\) so that \(u_i\) will not be performed but must be stored in \(L\) with the adjusted smaller values \(A, \beta_i\). The stored stages \(u_i\) with \(\beta_i ≥ 2^{−s}\) should be performed in a succession giving priority to large success rates and small \(t^∗\).

Time for solving SVP for \(\mathcal{L}(B)\). New Enum performs for each \(s = 5, 6, \ldots, s_{max}\) only stages \(u_i\) with success rate \(\beta_i ≥ 2^{−s}\). Let \(#\pi_{t,s,A}\) denote the number of performed stages with \(t, s, A\). If \(\beta_t\) is a reliable probability then New Enum performs on average at most \(2^t\) stages with success rate \(\beta_t ≥ 2^{−s}\) before decreasing \(A\) - this number of performed stages is even smaller than \(2^s\) since New Enum also performs stages with success rate \(\beta_t ≥ 2^{−s+1}\). New Enum performs for each stage of step 2 on average at most \(2(n - t)(1 + o(1))\) arithmetical steps for computing \(y_i\) which add up to \(\sum_{i=1}^n 2(n - t)(1 + o(1)) ≈ 2n^2\) arithmetical steps and it performs \(O(n)\) arithmetical steps for testing that \(\beta_t ≥ 2^{−s}\) for \(t = 1, \ldots, n\) using \(\beta_t ≈ V_{t−1}k−1/\det L\) assuming that \(\ln(2επ), \ln π, \ln(1 + x)\) for \(x = 1, \ldots, n\) are given for free.

If the initial basis \(B\) is a BKZ-basis with block size \(k\) then \(||b||\) ≤ \(\lambda_1 k^{n−1}. As New Enum performs stages with high success rates first then each decrease of \(A\) will on average halve \(A/\lambda_1^2\) so that there are at most \(log_2(A/\lambda_1^2)\) iterations of step 2 that decrease the initial \(A\) of step 1. So after the initial reduction of \(B\) New Enum solves SVP for \(s_{max}\) with error probability \(o(1)\) and performs on average at most \(O(n^2 s_{max})\) arithmetical steps for each \(A\). Hence SVP is solved by

\[2^{s_{max}}(2^s + O(n))t \frac{1}{2} \log_2 \gamma_k \text{ arithmetical steps.} \quad (3.2)\]

Pruned New Enum for CVP. Given a target vector \(t = \sum_{i=1}^n r_i b_i \in \mathcal{L}(B)\), \(\lVert t - b \rVert^2 \leq \frac{1}{4} \sum_{i=1}^n r_i^2\) in polynomial time for an LLL-basis \(B = QR, R = [r_{i,j}]\) holds.

Adoption of New Enum to CVP to find \(b \in \mathcal{L}(B)\) such that \(||t - b||^2 < A\). Initially we set \(\hat{A} := \frac{1}{2} \sum_{i=1}^n r_i^2\) so that \(||t - \hat{A}||^2 < \hat{A}\). Having found some \(b \in \mathcal{L}\) such that \(||t - b||^2 < \hat{A}\) New Enum gives out \(b\) and decreases \(\hat{A}\) to \(||t - b||^2\).

Optimal value of \(\hat{A}\). If the distance \(||t - \hat{L}||\) or a close upper bound of it is known then we initially choose \(\hat{A}\) to be that close upper bound. This prunes away many irrelevant stages. At stage \((u_i, \ldots, u_n)\) NEW ENUM searches to extend the current \(b = \sum_{i=1}^n u_i b_i \in \mathcal{L}\) to some \(b' = \sum_{i=1}^n u_i b_i \in \mathcal{L}\) such that \(||t - b'||^2 < \hat{A}\). The expected number of such \(b'\) is for random \(t\):

\[\hat{\beta}_t := \frac{1}{\hat{A} \cdot \pi_t(t - b||^2)^{1/2}} \text{ for } \hat{\beta}_t := (A - ||\pi_t(t - b||^2)^{1/2}.\]

Previously, stage \((u_{i+1}, \ldots, u_n)\) determines \(u_t\) to yield the next index minimum of
New Enum for CVP

INPUT BKZ-basis \( B = QR \in \mathbb{R}^{m \times n}, R = [r_{i,j}] \in \mathbb{R}^{n \times n}, t = \sum_{i=1}^{n} \tau_i b_i \in \text{span}(L), \tau_1, \ldots, \tau_n \in \mathbb{Q} \), a small \( A \in \mathbb{Q} \) such that \( \|t - L(B)\|^2 \leq \bar{A}, s_{\max} \).

OUTPUT A sequence of \( b = \sum_{i=1}^{n} u_i b_i \in L(B) \) such that \( \|t - b\|^2 \) decreases to \( \|t - L\| \).

1. Let \( n, L = \emptyset, y_n = \tau_n, u_n := |y_n|, \hat{e}_{n+1} := 0, s := 5 \) and \( c_i = c_i(\tau_i - u_i, \ldots, \tau_n - u_n) \) always holds for the current \( t, u_i, \ldots, u_n \).

2. WHILE \( t \leq n \) #perform stage \( u_i := (u_i, \ldots, y_n, c_i, \nu_i, \xi, \hat{\beta}_i, \hat{A}) \)

   \( \|\hat{e}_i : = \hat{e}_{i+1} + (u_i - y_i)^2 r_i^2, \)
   \( \| \)
   IF \( \hat{e}_i \geq \bar{A} \) THEN GO TO 2.1.
   \( \hat{b}_i := (\bar{A} - \hat{e}_i)^{1/2}, \hat{\beta}_i := \frac{r_i}{\hat{b}_i} (r_{i,1} \cdots r_{i-1,1}^{-1}) \).
   \( \| \)
   IF \( t = 1 \) THEN \( b := \sum_{i=1}^{n} u_i b_i \)
   \( \| \)
   IF \( \|t - b\|^2 < \bar{A} \) THEN [ \( \hat{A} := \|t - b\|^2, \text{output}(b, s, \hat{A}), \text{GO TO 2.1} \) ]
   \( \| \)
   \( \hat{\beta}_i \geq 2^{-s} \) THEN \( t := t - 1, y_i := \tau_i + \sum_{i=1}^{n} (\tau_i - u_i) r_{i,1} r_{i,t} \),
   \( \| \)
   \( u_i := |y_i|, \xi := \text{sign}(u_i - y_i), \nu_i := 1, \text{GO TO 2} \)
   \( \| \)
   \( \hat{\beta}_i \geq 2^{-s_{\max}} \) THEN store \( u_i := (u_i, \ldots, y_n, c_i, \nu_i, \xi, \hat{\beta}_i, \hat{A}) \) in \( L \).

3. perform all stages \( u_i := (u_i, \ldots, y_n, c_i, \nu_i, \xi, \hat{\beta}_i, \hat{A}) \) in \( L \) with \( \hat{\beta}_i \geq 2^{-s} \),
   \( \| \)
   IF steps 2, 3 did not decrease \( A \) for the current \( s \) THEN terminate.
   \( \| \)
   \( 4. s := s + 1, \text{IF } s > s_{\max} \text{ THEN restart with a larger } s_{\max}. \)

4 New Enum for SVP and CVP with linear pruning

The heuristics of linear pruning gives weaker results but is easier to justify than handling the success rate \( \beta \) as a probability function. Proposition 1 bounds under linear pruning the time to find \( b' \in L(B) \) with \( \|b'\| = \lambda_1 \). It shows that SVP is polynomial time if \( rd(L) \) is sufficiently small. Note that finding an unproved shortest vector \( b' \) is easier than proving \( \|b'\| = \lambda_1 \). New Enum finds an unproved shortest lattice vector \( b' \) in polynomial time under the following conditions and assumptions:

- the given lattice basis \( B = [b_1, \ldots, b_n] \) and the relative density \( rd(L) \) of \( L(B) \) satisfy \( rd(L) \leq \left( \frac{\sqrt{n} \lambda_1}{32 \pi} \right)^2 \), i.e., both \( b_1 \) and \( rd(L) \) are sufficiently small.

GSA: The basis \( B = QR, R = [r_{i,j}]_{i=1,j=1}^{n} \) satisfies \( \tau_{i,i} \leq \tau_{i-1,i-1} = q \) for \( 2 \leq i \leq n \) for some \( q > 0 \).

SA: There is a vector \( b' \in L(B) \) such that \( \|b'\| = \lambda_1 \) and \( \|\pi_i(b')\|^2 \leq \frac{n+1}{n} \lambda_1^2 \) for \( t = 1, \ldots, n \).

(Later we will use a similar assumption CA for CVP )

- the vol. heur. is close: \( M := \#B_{n-t+1}(0, q/t) \cap \pi_i(L) \approx \frac{\tau_{n-t+1}^{n-t+1}}{\det \pi_i(L)} \) for \( \hat{\rho} = \frac{n+1}{n} \lambda_1^2 \).

Remarks. 1. If GSA holds with \( q \geq 1 \) the basis \( B \) satisfies \( \|b_i\| \leq \sqrt{\frac{1}{3} + 3 \tau_i} \) for all \( i \) and \( \|b_1\| = \lambda_1 \). Therefore, \( q < 1 \) unless \( \|b_1\| = \lambda_1 \). GSA means that the reduction of the basis is "locally uniform", i.e., the \( \tau_{i,i} \) form a geometric series. It is easier to work with the idealized property that all \( \tau_{i,i} \) are equal. In practice, it slightly increases on the average with \( i \). [BL05] studies "nearly equality". B. LANGE [La13] shows that GSA can be replaced by the weaker property that the reduction potential of \( B \) is sufficiently small. GSA has been used in [S03, NS06, G08, S07, N10] and in the security analysis of NTRU in [H07, HHHW09].

2. The assumption SA is supported by a fact proven in the full paper of [GNR10]:

\[ \Pr[\|\pi_i(b')\|^2 \leq \frac{n+1}{n} \lambda_1^2] \] for \( t = 1, \ldots, n \) = \( \frac{1}{2} \)

for random \( b' \in \text{span}(L) \) with \( \|b'\| = \lambda_1 \). B. LANGE [La13, Kor. 4.3.2] proves that the prob. 1/n
increases to \(1 - e^{-d^2}\) by increasing \(\frac{n-t+1}{t}\) of linear pruning to \(\frac{n-t+1}{t} + d/\sqrt{n}\). Linear pruning means to cut off all stages \((u_1, ..., u_n)\) that satisfy \(\|\pi_t(\sum_{i=1}^n u_i b_i)\|^2 > \frac{n-t+1}{t}\lambda^2\). Linear pruning is impractical because it does not provide any information on SVP, CVP in case of failure. We use linear pruning only as a theoretical model for easy analysis. We have implemented SVP, CVP via New Enum and we will show in section 5 that stages \((u_1, ..., u_n)\) that are cut by linear pruning have extremely low success probability so they will not be performed by New Enum.

3. Errors of the volume heuristics. The minimal and maximal values of \#_{a} := \#((B, \zeta, \rho) \cap \mathcal{L})\) and similar for \#_{t} := \#((B, \zeta, \rho) \cap \pi_{n-t+1}(\mathcal{L}))\), are for fixed \(n, \rho\) very close for large radius \(\rho\), but can differ considerably for small \(\rho\) since \#_{a} can change a lot with the actual center \(\zeta\) of the sphere. For small \(\rho\), the minimum of \#_{a} can be very small and then the average value for random center \(\zeta\) is closer to the maximum of \#_{a}. For more details see the theorems and Table 1 of [MO90]. As New Enum works with average values for \#_{a}, \#_{t} its success rate \(\beta\) frequently overestimates the success rate for the actual \(\zeta\). A cut of the smallest (resp. closest) lattice vector by New Enum in case that it underestimates \#_{t} can nearly be excluded if stages are only cut for very small \(\beta\).

4. A trade-off between \(\|b_{1}\|/\lambda_{1}\) and \(rd(\mathcal{L})\) under \textbf{GSA}. B. Lange observed that

\[
\|b_{1}\|/\lambda_{1} = \|b_{1}\|/(rd(\mathcal{L})\sqrt{n}) det(\mathcal{L})^{1/2} = q^{\frac{1-n}{2}}/(rd(\mathcal{L})\sqrt{n}).
\]

Therefore \(rd(\mathcal{L})\sqrt{n}/\|b_{1}\|/\lambda_{1} \leq 1\) implies under \textbf{GSA} that \(det(\mathcal{L}) \geq 1\) and \(q \geq 1\) and thus \(\|b_{1}\| = \lambda_{1}\). Hence \(rd(\mathcal{L}) > \|b_{1}\|/\sqrt{n}\) holds under \textbf{GSA} if \(\|b_{1}\| > \lambda_{1}\).

Our time bounds must be multiplied by the worst polynomial factor covering the steps performed at stage \((u_1, ..., u_n)\) of Enum before going to a subsequent stage.

**Proposition 1.** Let the basis \(B = QR, R \in \mathbb{R}^{n \times n}\) of \(\mathcal{L}\) satisfy \(rd(\mathcal{L}) \leq (\frac{\lambda_{1}}{\gamma_{n}})^{n} \frac{1}{\sqrt{n}}\) and \(\textbf{GSA}\) and let \(\mathcal{L}\) have a shortest lattice vector \(b'\) that satisfies \(\textbf{SA}\). Then Enum with linear pruning finds such \(b'\) under the volume heuristics in polynomial time.

**Proof.** For simplicity we assume that \(\lambda_{1}\) is known. Pruning all stages \((u_1, ..., u_n)\) that satisfy \(\|\pi_t(\sum_{i=1}^n u_i b_i)\|^2 > \frac{n-t+1}{t}\lambda^2\) does not cut off any shortest lattice vector \(b'\) that satisfies \(\textbf{SA}\). The volume heuristics approximates the number \(M_{t}\) of performed stages \((u_1, ..., u_n)\) to

\[
M_{t} = \#B_{n-t+1}(0, \rho) \cap \pi_t(\mathcal{L}) \approx (\frac{n-t+1}{t}\lambda_{1})^{n-t+1}V_{n-t+1}/(r_{1,t} \cdots r_{n,n})
\]

\[
\approx (\frac{n-t+1}{t}\lambda_{1})^{n-t+1}(\frac{2n}{n-t+1})^{\frac{n-t+1}{2}}/(r_{1,t} \cdots r_{n,n} \sqrt{\pi(n-t+1))})
\]

\[
< (\lambda_{1}\sqrt{\frac{2\pi}{n}})^{n-t+1}/(r_{1,t} \cdots r_{n,n}).
\]

(4.1)

Here \(\approx\) uses Stirling’s approximation \(V_{n} = \pi^{n/2}/(n/2)! \approx (\frac{2\pi}{n})^{n/2}/\sqrt{n}\). Obviously \(\|b_{1}\| = r_{1,1}q^{\frac{1}{2}}\) holds by \(\textbf{GSA}\) and thus

\[
(r_{1,t} \cdots r_{n,n})/r_{1,1}^{n-t+1} = q^{\gamma_{n-1}-(t-1)(t-2)}.
\]

For \(t = 1\) this yields \(\frac{n-1}{t} = (det(\mathcal{L}))^{1/n}/r_{1,1} = \lambda_{1}/(r_{1,1}\sqrt{n}rd(\mathcal{L}))\). Combining (4.1) with this equation and \(\gamma_{n} < \frac{n}{2}\) which holds for \(n > n_{0}\), we get

\[
M_{t} \leq (\frac{\lambda_{1}}{\gamma_{n}})^{n} \frac{1}{\sqrt{n}} rd(\mathcal{L})^{\frac{n}{2}} \lambda_{1}^{n-1} (\frac{2\pi}{n})^{\frac{n-t+1}{2}} \sqrt{\pi(n-t+1))}
\]

(4.2)

Evaluating this upper bound for \(rd(\mathcal{L}) \leq (\frac{\lambda_{1}}{\gamma_{n}})^{n}\sqrt{\pi(n-t+1)}\) yields

\[
M_{t} \leq (\frac{\lambda_{1}}{\gamma_{n}})^{n} \frac{1}{\sqrt{n}} (\frac{2\pi}{n})^{n-t+1} \frac{1}{\sqrt{\pi(n-t+1))}} \approx (\frac{2\pi}{n})^{n-t+1} (\frac{2\pi}{n})^{n-t+1} \frac{1}{\sqrt{\pi(n-t+1))}}
\]

This approximate upper bound has for \(t \leq n\) its maximum 1 at \(t = n\). This proves Prop. 1. \(\square\)

**Extension of Prop. 1 to \textbf{GSA}_{m,q}\)-bases.** i.e. lattice bases that satisfy for some \(m, 1 \leq m \leq n :\)

\[
r_{i,i}/r_{i-1,i-1} = \begin{cases} q & \text{for } i \leq m, \\ 1 & \text{for } i > m \end{cases}, \\
q^{-1} & \text{for } i \leq m, \\
q^{m-1} & \text{for } i > m
\]

This increases \(r_{i,i}/r_{i-1,i-1}\) of \textbf{GSA} for \(i \geq m\); many LLL-bases have such an increase for large \(i\).
Proposition 2. Let $B = QR, R \in \mathbb{R}^{n \times n}$ be a GSA$_{m,n}$-basis, $rd(L(B)) \leq \frac{1}{\sqrt{n}}(\frac{\lambda_1}{\pi}B\sqrt{\frac{2\pi}{n}})^m$ and $L$ have a shortest lattice vector $b'$ that satisfies SA. Then Enum with linear pruning finds such $b'$ under the volume heuristics in polynomial time.

Proof. We modify the proof of Prop. 1 and concentrate on $t \geq m$ since $M_t^{\lambda}$ has its maximum for $t \geq m$. Then we have for $t \geq m$

$$ (r_{1,t} \cdots r_{n,n})/r_{1,1}^{n-t+1} = q^{(n-t+1)\frac{n-m}{2}} $$

$$(\det L)^{1/n}/r_{1,1} = q^{\sum_{j=1}^{n-1} \frac{i-j}{n} + \frac{m-1}{n} - \frac{m-1}{2} \frac{n-m}{2}} = \frac{\lambda_1}{r_{1,1}}\sqrt{\frac{2\pi}{n}} rd(L) $$

where

$$ \sum_{j=1}^{n-1} \frac{i-j}{n} + \frac{m-1}{n} - \frac{m-1}{2} \frac{n-m}{2} = \frac{m-1}{2} (1 - \frac{m}{n}). $$

Hence

$$ M_t^{\lambda} \approx (\frac{\lambda_1}{r_{1,1}}\sqrt{\frac{2\pi}{n}})^{n-t+1}/q^{(n-t+1)\frac{n-m}{2}} = (\frac{\lambda_1}{r_{1,1}}\sqrt{\frac{2\pi}{n}})^{n-t+1} (\frac{\lambda_1}{r_{1,1}}\sqrt{\frac{2\pi}{n}} rd(L))^{n-m/2} $$

Evaluating $\frac{r_{1,1}}{r_{1,1}}\sqrt{\gamma_r} rd(L)$ for $rd(L) \leq \frac{1}{\sqrt{n}}(\frac{\lambda_1}{\pi}B\sqrt{\frac{2\pi}{n}})^m$ and $\gamma_n \leq \frac{\lambda_1}{2}$ we get

$$ M_t^{\lambda} \approx \left(\frac{\lambda_1}{r_{1,1}}\sqrt{\frac{2\pi}{n}}\right)^{(1-\frac{n-m}{n}(1-\frac{m}{n}))^{n-m/2}} = \left(\frac{\lambda_1}{r_{1,1}}\sqrt{\frac{2\pi}{n}}\right)^{n-m/2} $$

and thus

$$ M_t^{\lambda} \leq \left(\frac{\lambda_1}{r_{1,1}}\sqrt{\frac{2\pi}{n}}\right)^{(1-\frac{n-m}{n}(1-\frac{m}{n}))^{n-m/2}} \leq 1. $$

In particular $M_t^{\lambda} \approx 1$ holds for all $t \geq m$ if $rd(L) = \frac{1}{\sqrt{n}}(\frac{\lambda_1}{\pi}B\sqrt{\frac{2\pi}{n}})^m$ and $\gamma_n = \frac{\lambda_1}{2}$. $\square$

Prop 2 handles the case that $r_{i,i}$ decreases uniformly for $i \leq m$ with an abrupt stop at $i = m$. Prop 3 assumes a lattice basis of dimension $n$ that satisfies for some $0 < q < 1$ that

$$ r_{i+1,i+1}/r_{1,1} = q^{1-i/n} \quad \text{for} \quad i = 1, \ldots, n-1 $$

(4.3)

Hence $r_{j,j}/r_{1,1} = q^{1-\Sigma_{i=1}^{j-1}/n}$ and $r_{i,i}$ decreases slower and slower from $i = 1$ to $i = n$ and the decrease vanishes for $i \approx n$. In fact for LLL-bases the decrease of $r_{i,i}$ can vanish slowly towards the end of the basis because the LLL-algorithm works uniformly on the initial part but merely perfumes size-reduction towards the end of an high-dimensional basis.

Proposition 3. Let $B = QR, R \in \mathbb{R}^{n \times n}$ be a basis of lattice $L$ satisfying (4.3), $n > 4\pi e$ and $rd(L) \leq (\frac{\pi}{4\pi e})^{1/2}$ and let $L$ have a shortest lattice vector $b'$ that satisfies SA. Then Enum with linear pruning finds such $b'$ under the volume heuristics in polynomial time.

Proof. Modifying the proofs of Prop.1, 2 we have

$$ r_{i,t} \cdots r_{n,n}/r_{1,1}^{n-t+1} = q^{\sum_{j=1}^{n} j - (n-1)/2} = \frac{n(n+1)}{2} - \frac{(n-1)(n-2)}{2} \frac{2n}{n} $$

Hence

$$ \left(\frac{\lambda_1}{r_{1,1}}\sqrt{\frac{2\pi}{n}}\right)^{n-t+1} = \det L/r_{1,1}^{n-t+1} = q^{n^2/3 + O(n)}. $$

This bounds the number $M_t^{\lambda}$ of performed stages $(u_1, \ldots, u_n)$ under linear pruning to

$$ M_t^{\lambda} \approx \left(\frac{\lambda_1}{r_{1,1}}\sqrt{\frac{2\pi}{n}}\right)^{n-t+1} (\det L)^{1/n}/r_{1,1} \approx \frac{\lambda_1}{r_{1,1}}\sqrt{\frac{2\pi}{n}}^{n-t+1} q^{-n^2/3} \frac{2n}{n} \frac{2n}{n} + O(n) $$

$$ \approx \frac{\lambda_1}{r_{1,1}}\sqrt{\frac{2\pi}{n}}^{n-t+1} \frac{2n}{n} \frac{2n}{n} + O(n) $$

We get for $rd(L) \leq (\frac{\pi}{4\pi e})^{1/2}$ and $\gamma_n = \frac{\lambda_1}{2}$ that $r_{1,1}^2 \sqrt{\gamma_r} rd(L)/\lambda_1 \approx (\frac{\lambda_1}{r_{1,1}}\sqrt{\frac{2\pi}{n}})^{1/2}$ and thus

$$ M_t^{\lambda} \leq \left(\frac{\lambda_1}{r_{1,1}}\sqrt{\frac{2\pi}{n}}\right)^{n-t+1} - (2n-1) \frac{2n}{n} \frac{2n}{n} + O(n) $$

$$ \leq \left(\frac{\lambda_1}{r_{1,1}}\sqrt{\frac{2\pi}{n}}\right)^{n-t+1} - \frac{2n}{n} \frac{2n}{n} + O(n) $$

For $n > 4\pi e$ this upper bound $H_t$ of $M_t^{\lambda}$ is monotonous decreasing in $t \leq n$. This holds because the exponent of $\frac{\lambda_1}{r_{1,1}}\sqrt{\frac{2\pi}{n}}^{n-t+1}$ is monotonous increasing in $t$ and $\frac{\lambda_1}{r_{1,1}}\sqrt{\frac{2\pi}{n}} < 1$. Hence for $n > 4\pi e$

$$ M_t^{\lambda} \leq \frac{\lambda_1}{r_{1,1}}\sqrt{\frac{2\pi}{n}}^{n-t+1} - \frac{2n}{n} \frac{2n}{n} + O(n) $$

$$ \leq \frac{\lambda_1}{r_{1,1}}\sqrt{\frac{2\pi}{n}}^{n-t+1} - \frac{2n}{n} \frac{2n}{n} + O(n) $$

In practice all relevant bases satisfy some slightly modified version of GSA. The main problem for the fast SVP algorithms for them is to find a sufficiently short $b_1 \in L$. For this we first iteratively BKZ-reduce the basis $B$ with block sizes 2, 4, 8, 16, 32 and then for larger block sizes we use NEW
Enum with pruning and arranged to enumerate smallest vectors first.

The $\gamma$-unique SVP is to solve SVP for a lattice $\mathcal{L}$ of dim. $n$ where $\lambda_2 \geq \gamma \lambda_1$ holds for the second successive minimum $\lambda_2$, Minkowski’s second theorem shows for such $\mathcal{L}$ with successive minima $\lambda_1, \ldots, \lambda_n$ that

\[ \lambda_1^{n-1} \leq \gamma^{1/n} \det \mathcal{L} \]

and thus

\[ \lambda_1^2 \leq \gamma^{2+1/n} \lambda_2 \det \mathcal{L} \]

Prop. 3 shows that SVP for such $\mathcal{L}$ is solvable in polynomial time under SA, GSA and the volume heuristic if

\[ \lambda_1^{(n-1)}(k-1)^{1/k} \leq \sqrt{2/e} \gamma^{1/n} \]

has been proved that every BKZ-basis of block size $k$ satisfies $\|b_i\| / \lambda_1 \leq \gamma^{(n-1)/(k-1)}$. Hence the heuristic pol. time for $n$-unique SVP holds if

\[ \lambda_1^{(n-1)} \leq \gamma^{1/n} \sqrt{2/e} \gamma^{1/n} \]

The latter holds for

1. $\lambda_1 = 2a$, $\lambda_2 = 4$ for all $n \leq 245$
2. $\lambda_1 = 2a$, $\lambda_2 = 4$ for all $n \leq 140$

We see that the security of cryptosystems based on $n$-unique SVP is quite weak for practical, not extremely large dimension $n$. For cryptosystems based on $n$-unique SVP see [Reg04], [MR05].

**SVP-time bound for $rd(L) \leq 1$ under linear heuristic.** (4.2) proves for $rd(L) \leq 1$ that

\[ M_n \leq \left( \sqrt{\frac{n^2}{\pi}} \right) \frac{1}{\gamma} \frac{2^{n/4}}{n^4} \]

This beats under the heuristic the proven SVP time bound $n^{17+o(n)}$ of HANROT, STEHLE [HS07] which holds for a quasi-HKZ-basis $B$ satisfying $\|b_i\| \leq 2\|b_2\|$ and having a HKZ-basis $\pi_2(B)$. In fact $\frac{1}{\gamma} \approx 0.159 > 0.125 = \frac{1}{2}$. The SVP-algorithm of Prop.1 can use fast BKZ for preprocessing and works even for $\|b_i\| \gg \lambda_1$ – see the attack on $\gamma$-unique SVP – whereas [HS07] requires quasi-HKZ-reduction for preprocessing. This eduction already guarantees $\|b_i\| \leq 2\lambda_1$ and performs the main SVP work during preprocessing. Our SVP time bound $n^{8+o(n)}$ only assumes $\|b_i\| \leq n^{1/2} \lambda_1$.

**Theorem 1.** Given a lattice basis $B \in \mathbb{Z}^{m \times n}$ satisfying GSA and $\|b_i\| \leq \sqrt{\pi n} n^b \lambda_1$ for some $b \geq 0$, NEW ENUM solves SVP and proves to have found a solution in time $2^{O(n)} n^{1+o(n)}$. (4.4)

Theorem 1 is proven in [S10], it does not assume SA and the vol. heuristic. Recall from remark 4 that $n^{1/2+rd(L)} \geq 1$ holds under GSA. For $b = o(1)$ Thm. 1 shows the SVP-time bound $n^{17+o(n)}$ from HANROT, STEHLE [HS07]. Cor. 1 translates Thm. 1 from SVP to CVP, it shows that the corresponding CVP-algorithm solves many important CVP-problems in simple exponential time $2^{O(n)}$ and linear space. [HS07] proves the time bound $n^{17+o(n)}$ for solving CVP by KANNAN’s CVP-algorithm [Ka87]. Minimizing $\|b\|$ for $b \in \mathcal{L} \setminus \{0\}$ and minimizing $\|t - b\|$ for $b \in \mathcal{L}$ require nearly the same work if $\|t - \mathcal{L}\| = \lambda_1$. In fact the proof of Theorem 1 yields:

**Corollary 1.** [S10] Given a basis $B = [b_1, \ldots, b_n]$ satisfying GSA, $\|b_i\| \leq \sqrt{\pi n} n^b \lambda_1$ with $b \geq 0$ and $t \in \text{span} \mathcal{L}$ with $\|t - \mathcal{L}\| \leq \lambda_1$, NEW ENUM solves this CVP in time $2^{O(n)} n^{1/2+rd(L)} \frac{\lambda_1}{\sqrt{n}}$.

Corollary 1 proves under GSA, $rd(L) = O(n^{1/2-b})$ and $\|t - \mathcal{L}\| \leq \lambda_1$ the CVP time bound $2^{O(n)}$ even using linear space (by iterating NEW ENUM for $s = 1, \ldots, O(n)$ without storing delayed stages). Moreover it proves under GSA and $\|b_i\| = O(\lambda_1)$ and $\|t - \mathcal{L}\| \leq \lambda_1$ the time bound $2^{O(n)}$. However subexponential time remains unprovable due to remark 4 of section 4.

**CA:** $\|\pi_t(t - \hat{b})\|^2 \approx \frac{n+1}{n+1} \|t - \mathcal{L}\|^2$ holds for $t = 1, \ldots, n$ and some $\hat{b} \in \mathcal{L}$ closest to $t$.

CA translates the assumption SA from SVP to CVP. CA holds with probability $1/n$ for random $\hat{b} \in \text{span} \mathcal{L}$ such that $\|t - \hat{b}\| = \|t - \mathcal{L}\|$ [GNR10]. Obviously linear pruning extends naturally from SVP to CVP. B. LANDG [La13] proves that the probability $1/n$ increases towards 1 for the increased bounds $\|\pi_t(t - \hat{b})\|^2 \approx \frac{n+1}{n+1} (1 + 1/\sqrt{n})$ for $t = 1, \ldots, n$. 

8
Corollary 2. [S10] Given a basis \(B = \{b_1, \ldots, b_n\} \in \mathbb{Z}^{n \times n}\) of \(L\) that satisfies GSA, \(\|b_i\| = O(\lambda_i)\) and \(rd(L) \leq (\frac{\lambda_i}{|b_i|} \sqrt{|b_i|^2})^{\frac{1}{2}}\). Let some lattice vector \(b\) that is closest to the target vector \(t\) satisfy CA then New Enum finds \(b\) for random \(t\) in average time \(nO(1)E_b[||t - L||/\lambda_i^n]^{\frac{1}{2}}\).

Cor. 2 eliminates the volume heuristics for a random target vector \(t\). Prop. 1 translates into

Corollary 3. Let a basis \(B = \{b_1, \ldots, b_n\} \in \mathbb{Z}^{n \times n}\) of \(L\) be given satisfying GSA, \(\|b_i\| = O(\lambda_i)\) and 

\[ rd(L) \leq (\frac{\lambda_i}{|b_i|} \sqrt{|b_i|^2})^{\frac{1}{2}}. \]

Let some \(b \in L\) closest to the target vector \(t\) satisfy CA and let \(|t - L| \leq \lambda_i\) then Enum with linear pruning for CVP finds \(b\) under the volume heuristics in \(O(1)\) time.

B. LANGE [La13] shows that GSA for \(B\) can be replaced by a less rigid condition, namely that the “reduction potential” \(\prod_{i \geq 1} \ell_i\) for \(\ell_i = \|b_i\|/(\det L)^{1/n}\) of the basis \(B\) is sufficiently small.

Next we study the success rate \(\beta_i\) of stages \((u_1, \ldots, u_n)\) that are near the limit of linear pruning \(\|\pi_i(\sum_{j=1}^n u_ib_j)\|^2 \approx \frac{n+1}{n} n^2\). Following the proof of Prop. 1 the volume heuristics evaluates the expected number of successful extensions \((u_1, \ldots, u_{n-1})\) of \((u_1, \ldots, u_n)\) at this pruning limit to

\[ V_{n-1} \left( \frac{\lambda_i}{n} \right) \approx \frac{\lambda_i^{n-1}}{(n-1)!} \approx \frac{n-1}{\sqrt{n} \pi(n-1)} \]

Hence stage \((u_1, \ldots, u_n)\) has the success rate \(\beta_i \approx \frac{\lambda_i^{n-1}}{(n-1)!} \left( \frac{\sqrt{n} \pi(n-1)}{\lambda_i^2} \right)^{\frac{1}{2}} / \sqrt{n} \).

where \(r_1 \cdots r_{n-1} = \det(L([b_1, \ldots, b_{n-1}]))\) and we have due to GSA that

\[ r_1 \cdots r_{n-1} = \sqrt{\frac{\pi}{n-1}} \lambda_i \cdot \left( \frac{\sqrt{n} \pi(n-1)}{\lambda_i^2} \right)^{\frac{1}{2}}. \]

Hence \(\beta_i \approx \frac{\lambda_i^{n-1}}{(n-1)!} \left( \frac{\sqrt{n} \pi(n-1)}{\lambda_i^2} \right)^{\frac{1}{2}} / \sqrt{n} \).

We get for \(n \approx 10^{14}, n = 48, p_n = 223, c = 0.8468, r_1, r_2 \geq \lambda_i\) that

\[ \beta_{12} \approx 1.85 \times 10^{-5} \lambda_i^{5.5} r_1^{-0.866}, \quad \beta_{24} \approx 3.77 \times 10^{-20} \lambda_i^{11.5} r_1^{-12.23}, \quad \beta_{36} \approx 5.89 \times 10^{-41} \lambda_i^{17.5} r_1^{-9.68}. \]

Thus New Enum performs under linear pruning many stages with unreasonable small success rate. Cutting these stages by pruning saves time and space.

Enum with linear pruning solves SVP of \(L\) of dim \(L = n\) by (4.4) in worst case heuristic time \(n^{n/8+o(1)}\), New Enum solves SVP much faster. Short vectors are found much faster if available stages with large success rate are always performed first and if stages with very small success rate are cut. Our experiments show that New Enum for \(n \approx 10^{14}, 10^{20}\) and \(n = 90,150\) finds vectors in \(L(B_{n,c})\) close to \(N_c\) in polynomial time.

5 Factorizing by CVP solutions for the Prime Number Lattice

Let \(N > 2\) be an odd integer that is not a prime power and with all prime factors larger than \(p_n\), the \(n\)-th smallest prime. Then the \(p_i\) with \(i \leq n\) have inverses \(p_i^{-1}\) mod \(N\) in \(\mathbb{Z}/N\mathbb{Z}\). An integer is \(p_n\)-smooth if it has no prime factor larger than \(p_n\). A classical method factors \(N\) via \(n + 1\) independent pairs of \(p_n\)-smooth integers \(u, v\) such that \(|u - vN| \neq 0\) since \(N\) is not \(p_n\)-smooth, and \(u, v\) yields a fac-relation.

The classical factorization. Given \(n + 1\) fac-relations \((u_j, v_j)\) we have for \(p_0 := -1\)

\[ u_j = \prod_{i=1}^{n} p_i^{e_{i,j}}, \quad u_j - v_j N = \prod_{i=0}^{p_0} p_i^{e_{i,j}} \text{ with } e_{i,j}, e_{i,j}' \in \mathbb{N}. \]  

(5.1)

We have \((u_j - v_j N)/u_j \equiv 1\) mod \(N\) since \(\frac{1}{p_0} N \equiv 0\) mod \(N\) holds due to gcd\((N, u_j) = 1\). Hence

\[ \prod_{i=0}^{p_0} p_i^{e_{i,j}' - e_{i,j}} \equiv 1 \text{ mod } N. \]

Any solution \(t_1, \ldots, t_{n+1} \in \{0, 1\}\) of the equations

\[ \sum_{j=1}^{n+1} t_j (e_{i,j} - e_{i,j}') \equiv 0 \text{ mod } 2 \text{ for } i = 0, \ldots, n \]

(5.2)

solves \(X^2 - 1 = (X - 1)(X + 1) \equiv 0\) mod \(N\) by \(X = \prod_{i=0}^{p_0} p_i^{\sum_{j=1}^{n+1} t_j (e_{i,j}' - e_{i,j})}\) mod \(N\). In case \(X \neq \pm 1\) mod \(N\) yields two non-trivial factors gcd\((X \pm 1, N) \notin \{1, N\}\) of \(N\).
Lemma 5.3 of [MG02] proves that
\[ \lambda \sum \] for \( N \) reduces factoring \( N \) to finding about \( n + 1 \) \( p_n \)-smooth integers \( u, v - N \). This factoring method goes back to Morrison & Brillhart [MB75] and let to the first factoring algorithm in subexponential time by J. Dixon [D81].

We construct \( p_n \)-smooth triples \( u, v, |u - v N| \) from CVP solutions for the prime number lattice \( \mathcal{L}(B_{n,e}) \) with basis \( B_{n,e} = [b_1, \ldots, b_n] \in \mathbb{R}^{(n+1) \times n} \) and target vector \( N_e \in \mathbb{R}^{n+1} \) for some \( c > 0 \):

\[
B_{n,e} = \begin{bmatrix}
\sqrt{\ln p_1} & 0 & 0 \\
0 & \ddots & 0 \\
0 & 0 & \sqrt{\ln p_n}
\end{bmatrix}, \quad N_e = \begin{bmatrix}
0 \\
\vdots \\
0 \\
N^c \ln p_1 & \cdots & N^c \ln p_n
\end{bmatrix},
\]

(5.3)

\[
(\det \mathcal{L}(B_{n,e}))^2 = (\prod_{i=1}^n \ln p_i) (1 + N^{2c} \sum_{i=1}^n (\ln p_i)^2),
\]

(\det \mathcal{L}(B_{n,e}))^{2/n} = \ln p_n \cdot N^{2c/n} \cdot (1 + o(1))

\[
(\det \mathcal{L}(B_{n,e})) = \prod_{i=1}^n \sqrt{\ln p_i} \cdot N^c \ln N
\]

(5.4)

for \( \mathcal{L}_{n,e} = \mathcal{L}[B_{n,e}, N_e] \) and \( \ln = \log_2 \approx \log_{10} \). The prime number theorem shows \( \prod_{i=1}^n \ln p_i / \ln p_n = 1 - o(1) \) for \( n \to \infty \). By definition let \( o(1) \to 0 \) for \( n, N \to \infty \). We identify each vector \( b = \sum_{i=1}^n e_i b_i \in \mathcal{L}(B_{n,e}) \) with the pair \( (u, v) \) of relative prime and \( p_n \)-smooth integers

\[
u = \prod_{i > 0, P_i \not\mid v} e_i, \quad v = \prod_{i \leq 0, P_i \not\mid v} e_i \in N \quad \text{denoting } b \sim (u, v).
\]

For \( b \sim (u, v) \) we denote \( \delta_b := N^c \nu, \delta_{b-N_e} := N^c \nu \nu \) the last coordinates of \( b \) and \( b - N_e \).

As a factor \( p_i^{b_i} \) of \( u \) adds \( \pm e_i \ln p_i \) to \( v \) and \( \ln \nu \) to \( \|b\|^2 \) we have \( \|b\|^2 \geq \ln uv + \delta_b^2 \) with equality if and only if \( uv \) is squarefree so that \( e_i \in \{-1, 0, 1\} \) for all \( i \). \( \|b\|^2 \) and \( \ln uv + \delta_{b-N_e} \) are almost equal if \( \sum_{i \in \{-0,1\}} e_i \ln p_i / (\sum_{i \in \{-0,1\}} e_i \ln p_i) = o(1) \). Similarly

Fact 1. \( \|b - N_e\|^2 \geq \ln uv + \delta_{b-N_e}^2 \) holds for \( (u, v) \sim b \in \mathcal{L}(B_{n,e}) \) with equality iff \( uv \) is square-free.

Moreover \( \|\mathcal{L}(b) - N_e\|^2 \) is close to \( \ln uv + \delta_{b-N_e}^2 \) if \( uv \) is nearly square-free.

Lemma 1. We have \( \delta_{b-N_e} = N^c \ln(\sqrt{\nu}) = -N^c \sum_{i=1}^{\infty} (-x)^i / i \) for \( (u, v) \sim b \in \mathcal{L}(B_{n,e}) \) and \( x = \frac{u-vN}{2N} \in [-\frac{1}{2}, \frac{1}{2}] \). Then \( |u - vN| < vN^{1-c} \delta_{b-N_e} / (1 - \varepsilon/2) \) holds if either \( vN < u < vN(1+\varepsilon) \) or \( u < vN < u(1+\varepsilon) \). Let \( \|b - N_e\| = \lambda_1(\mathcal{L}_{n,e}) \) then \( \delta_{b-N_e} \leq \lambda_1(\mathcal{L}_{n,e}) \) and if \( \delta_{b-N_e}^2 \) is bounded by the average of the quadratic coordinates of \( b \) we even have \( \delta_{b-N_e} \leq \lambda_1(\mathcal{L}_{n,e}) / \sqrt{1 + \varepsilon} \).

Proof. We apply the Taylor form \( \ln(1+x) = \sum_{j=1}^{\infty} (-x)^j / j \) holding for \( x \in [-\frac{1}{2}, 1] \). Clearly \( \delta_{b-N_e} \) lies between the sums \( -N^c \sum_{i=1}^{\infty} (-x)^j / j \) for \( j = 1, 2 \).

If \( vN < u < (1+\varepsilon)u \) then

\[
\delta_{b-N_e} = N^c \frac{vN-u}{2N} \left(1 - \frac{vN-u}{2N} \right) < \delta_{b-N_e},
\]

and this implies

\[
u = \frac{vN-u}{2N} \left(1 - \frac{vN-u}{2N} \right) < \delta_{b-N_e}.
\]

If \( u < vN < (1+\varepsilon)u \) then

\[
\delta_{b-N_e} = N^c \frac{u-vN}{2N} \left(1 - \frac{u-vN}{2N} \right) < \delta_{b-N_e},
\]

and this implies

\[
u = \frac{u-vN}{2N} \left(1 - \frac{u-vN}{2N} \right) < \delta_{b-N_e}.
\]

Next we consider factoring of \( N \approx 10^{14} \) and \( N \approx 10^{20} \) by SVP algorithms for \( \mathcal{L}_{n,e} \).

Lemma 5.3 of [MG02] proves that \( \lambda_1^2 > 2c \ln N \) holds if the prime 2 is excluded from the prime basis. Lemma 2 extends this proof to include the prime 2 and increases the lower bound by \( 1 - o(1) \).

Lemma 2. \( \lambda_1^2 > 2c \ln N + 1 - \frac{1}{N^c - \varepsilon} \) holds for \( \mathcal{L}(B_{n,e}) \) where \( \lambda_1 = \|b\|, b \sim (u, v, \sqrt{uv}) = N^c - \varepsilon \).

Proof. Let \( b = B_{n,e}u \neq 0 \) be a shortest vector of \( \mathcal{L}(B_{n,e}) \), corresponding to \( (u, v) \). Let \( u > v \), otherwise replace \( b \) by \( -b \) which permutes \( u, v \). Then \( \ln \frac{\nu}{\nu} \) minimizes for some \( u \geq v + 1 \) hence

\[
\ln \frac{\nu}{\nu} \geq \ln(1 + (1 + v)) \quad \text{since } u \geq v + 1 \quad \text{and } \sqrt{uv} > v 
\]

\[
= \ln(1 + v) = \ln(1 + (1 + v)) 
\]

since \( \ln(1 + x) = -\sum_{i=1}^{\infty} (-x)^i / i \) for \( x \in (-1, 1) \).

Hence \( \lambda_1^2 \geq \ln uv + N^{2c} \ln^2 \left( \frac{\nu}{\nu} \right) \geq \ln uv + N^{2c} \frac{1}{2N^c} \left(1 - \frac{1}{2N^c} \right)^2 \geq f(\sqrt{uv}) \) where \( N^c \ln \frac{\nu}{\nu} = \delta_b \) is the last coordinate of \( b \). We abbreviate \( h := \sqrt{uv} \). The derivative \( \frac{df(\nu)}{d\nu} = h^{-5} \left(2h^4 + N^{2c}[-2h^2 + 3h - 1] \right) \)

10
is zero for some $h$ with $N^c - 0.751 < h < N^c - 0.75$, hence $h \approx N^c$ and this $h$ determines the minimal value $f(h)$ of $f$. Then the Lemma follows from

$$f(N^c - \varepsilon) = \ln((N^c - \varepsilon)^2) + \frac{N^{2c}}{(N^c - \varepsilon)^2} \left(1 - \frac{1}{2(N^c - \varepsilon)}\right)^2$$

$$= 2c\ln N + 2\ln(1 - \varepsilon/N^c) + \frac{1}{(1 - \varepsilon/N^c)^2} \left(1 - \frac{1}{2(N^c - \varepsilon)}\right)^2$$

$$\approx 2c\ln N + 1 - \frac{1}{2}N^c - O(N^{-2c}) \text{ for } |\varepsilon - 0.7505| \leq 10^{-3} \text{ by an easy proof.}$$

If $u = \prod_{i \geq 0} P_i^{e_i} = O(N^c)$, $u = v + 1$ with all $e_i \in \{-1, 0, 1\}$ then $\lambda_i^2 = 2c\ln N + O(1)$. Or else $\lambda_i^2$ increases by the minimum of $\eta_0^2 \geq N^{2c} \frac{\ln^2(\varepsilon)}{v^2}$ for $p_n$-smooth $v < u$ of order $u = O(N^c)$. □

Let $\Psi(X, y)$ denote the number of integers in $[1, X]$ that are $y$-smooth. Dickman [1930] shows

$$\lim_{y \to \infty} \Psi(y^z, y)y^{-z} = \rho(z) \quad \text{for any fixed } z > 0.$$  

$\rho(z)$ is the Dickman, De Bruin $\rho$-function, see [G08] for a recent survy. It is known that

$$\rho(z) = 1 \quad \text{for } 0 \leq z \leq 1, \quad \rho(z) = 1 - \ln z \quad \text{for } 1 \leq z \leq 2$$

$$\rho(z) = \left(\frac{\ln(1 + \frac{1}{y})}{\ln y}\right)^z = 1/z^{z+\sigma(z)} \text{ for } z \to \infty \quad (5.5)$$

Hildebrand [H84] extended (5.5) to a wide finite range of $y$ and $z$. For any fixed $\varepsilon > 0$

$$\Psi(y^z, y)y^{-z} = \rho(z) \left(1 + O\left(\frac{\ln(N^c)}{\ln y}\right)\right)$$

(5.6) holds uniformly for $1 \leq z \leq y^{1/2-\varepsilon}$, $y > 2$ if and only if the Riemann Hypothesis is true. Let $\Phi(N, p_n, \sigma)$ denote the number of triples $(u, v, |u - vN|) \in \mathbb{N}^3$ that are $p_n$-smooth and bounded as $v, |u - vN| \leq p_n^\sigma$. We conclude from (5.6) that

$$\Phi(N, p_n, \sigma) = \Theta(2p_n^{2\sigma} \rho\left(\frac{\ln(N^c)}{\ln p_n}\right)\rho^2(\sigma))$$

(5.7) uniformly holds for $\frac{\ln N}{\ln p_n} + \sigma \leq \frac{1}{2} - \varepsilon$ if the $p_n$-smoothness events of $u, v, |u - vN|$ are nearly statistically independent. We will use (5.7) in a range where $\frac{\ln N}{\ln p_n} + \sigma < \varepsilon/4$ and we will neglect the $\Theta(1)$-factor of (5.7).

**Proof of (5.7).** There are $2p_n^{\sigma}$ pairs of integers $u, v$ such that $0 < v, |u - vN| \leq p_n^\sigma$ clearly $u \leq Np_n^\sigma + p_n^\sigma \leq p_n^\sigma$ holds for $z = \frac{\ln(N^c + 1)}{\ln p_n} + \sigma$. Then (5.6) for $y^z = p_n^\sigma = (N + 1)p_n^\sigma$ shows that the fraction of $u$ that are $p_n$-smooth is $\rho(z)\left(1 + O\left(\frac{\ln(N^c)}{\ln p_n}\right)\right)$ if $\frac{\ln N}{\ln p_n} + \sigma \leq \varepsilon/4$. Moreover (5.6) for $y = p_n, z = \sigma$ shows that the fraction of $0 < v \leq p_n^\sigma$ that are $p_n$-smooth is $\rho(\sigma)\left(1 + O\left(\frac{\ln(N^c)}{\ln p_n}\right)\right)$ if $\sigma \leq \frac{1}{2} - \varepsilon$. Therefore the statistical independence of the $p_n$-smoothness events of $u, v, |u - vN|$ implies (5.7) if $\ln(z + 1) = O(\ln p_n)$ holds for both $\rho$-values. The latter holds due to $\frac{\ln N}{\ln p_n} + \sigma \leq \varepsilon/4$.

**Example factoring for small $v$**. Let $N = 1000000080001501 \approx 10^{14}$ and $n = 90, p_{90} = 463$, $c = 1/2$. (5.7) shows that there are $\Theta(6.4 \cdot 10^5)$ fac-relations such that $v, |u - vN| \leq 463^3$ are $p_n$-smooth. M. Charlet has constructed in 2013 several hundred such relations (5.1) for the above $N$ by the following program pruned to stages with success rate $\hat{\beta}_1 \geq 2^{-14}$. This program found on average a relation every 6.5 seconds. This amounts to a factoring time of 10 minutes. (Increasing $c$ from $1/2$ to $5/7$ did on average increase the $v$-values of the found relations (5.1) and of course the entries in the last row of $[\mathbf{B}_{v,c}, \mathbf{N}_c]$ that are multiples of $N^c$. However the average time for constructing a fac-relation decreased from 6.5 to 6.08 seconds.

**A program for finding relations (5.1) efficiently.** Initially the given basis $\mathbf{B}_{v,c}$ gets strongly BKZ-reduced with block size 32 and the target vector $\mathbf{N}_c$ is shifted modulo lattice vectors into the ground mesh of the reduced basis. The initial value $\tilde{A}$, the upper bound on $||\mathbf{N}_c - \mathcal{L}(\mathbf{B}_{v,c})||^2$ is set to $\frac{1}{4} \sum_{i=1}^{\tau^2} r_i^2$, which is $\frac{1}{4}$ of the standard upper bound. We can find more fac-relations by decreasing $\tilde{A}$ only to $||b - \mathbf{N}_c||^2(1 + \epsilon)$ for the closest found $b \in \mathcal{L}(\mathbf{B}_{v,c})$. This larger final $\tilde{A}$ increases all final success rates $\hat{\beta}_1$ and extends the final enumeration of $b$ with $||b - \mathbf{N}_c||^2 \leq \tilde{A}$.  

11
LOOP. After the first round the vectors of the reduced basis of \( \mathcal{L}(B_{n,c}) \) and the shifted \( N_c \) are randomly scaled as follows. For \( i = 1, \ldots, n \) with probability 1/2 all \( i \)-th coordinates of the basis vectors and the shifted target vector are multiplied by 2. (The "scaled" primes \( p_i \) will appear less frequently as factors of \( uv \) in relations (5.1) resulting from CVP-solutions.) The scaled basis gets slightly reduced by BKZ-reduction of block size 20. Then New Enum for CVP is called to search for lattice vectors that are close to the shifted target vector \( N_c \). New Enum always decreases \( A \) to the square distance to \( N_c \) of the closest found lattice vector. Whenever a fac-relation has been found New Enum stops further decreasing \( A \) for this round and continues to enumerate all \( b \in \mathcal{L}(B_{n,c}) \) such that \( |b - N_c|^2 \leq A \).

1. \( 2 \cdot 3 \cdot 17^2 \cdot 103 \cdot 263 \cdot 317 \cdot 379 \cdot 443 \)  
   12  

2. \( 2 \cdot 5 \cdot 47 \cdot 83 \cdot 157 \cdot 179 \cdot 307 \cdot 331 \cdot 421 \)  
   14  

3. \( 7^2 \cdot 13 \cdot 41 \cdot 43 \cdot 107 \cdot 109 \cdot 113 \cdot 131 \cdot 409 \cdot 461 \)  
   19  

4. \( 2 \cdot 7 \cdot 13 \cdot 31 \cdot 107 \cdot 127 \cdot 149 \cdot 179 \cdot 383 \cdot 397 \cdot 439 \)  
   21  

5. \( 43 \cdot 131 \cdot 139 \cdot 193 \cdot 307 \cdot 353 \cdot 401 \cdot 439 \)  
   28829  

6. \( 19 \cdot 31 \cdot 53 \cdot 61 \cdot 67 \cdot 131 \cdot 163 \cdot 241 \cdot 313 \)  
   2055  

7. \( 13^2 \cdot 17 \cdot 101 \cdot 137 \cdot 199 \cdot 229 \cdot 277 \cdot 331 \)  
   1661  

8. \( 19 \cdot 101 \cdot 107 \cdot 127 \cdot 131 \cdot 179 \cdot 191 \cdot 211 \cdot 379 \)  
   93398  

The first 10 fac-relations of rounds 6 - 33 for \( c = 1/2 \). They mostly satisfy \( v, |u - vN| \leq p^3_{90} \).

A. Schickendantz improved in 2015 Charlet’s program and found for \( N = 100000980001501 \approx 10^{14} \), \( n = 90 \), \( p_90 = 463 \), \( c = 1/2 \) and pruned to stages with \( \beta_i \geq 2^{-14} \) on average one relation (5.1) in 0.32 seconds. This factors \( N \approx 10^{14} \) in 30 seconds. He scaled a strong BKZ-basis of \( \mathcal{L}(B_{n,c}) \) by multiplying by 2 by the first \( n \) rows only with probability 1/4 and almost skipped to adjust success rates of the stored stages when \( A \) has been decreased. But for \( N \approx 10^{20} \) this program took for \( n = 150 \), \( c = 1/2 \) about 34.5 seconds per fac-relation and factored \( N \) in 86 minutes. As the running time for SVP increases quite fast for greater \( N \) and \( n \) we look for better algorithms.

Searching fac-relations with \( v \leq p_n \): We will in \( \mathcal{L}(B_{n,c}) \) find \( b \sim (u, v) \) with \( p_n \)-smooth \( |u - vN| \) using methods that are faster than SVP-algorithms for \( \mathcal{L}(B_{n,c}) \). When \( |u - vN| = p_n \) then \( z = \ln |u - vN|/\ln p_n \) and random \( |u - vN| \) are \( p_n \)-smooth with probability \( \rho(z) \). Let \( z = |z| + \varepsilon \) with \( 0 < \varepsilon < 1 \) then \( \rho(z) \approx \rho(|z|)(\rho(|z|)^{\varepsilon})^{\varepsilon} \).

Algorithm for factoring \( N \approx 2^{100} \) by lattice reduction of \( \mathcal{L}_{n,c} \) \( c = 1 \), \( n = 191 \), \( p_n = 1153 \):

1. LLL-reduce the basis \( [B_{n,1}, N_1] \), compute its GNF \( R = [r_{i,j}]_{1 \leq i,j \leq 122} \in \mathbb{R}^{192 \times 192} \) in pol. time.

2. Primal-dual reduce the basis \( R \) by algorithm 6.3.1 (script), where \( 192 = hk \), \( h = 192/k = 8 \) for \( k = 24 \), Theorem 6.3.2 (script) shows that this yields a vector \( b_i \in \mathcal{L}_{n,1} \) with \( |b_i|^2 \leq \gamma_k (\alpha^2) \sum_{j=1}^{k-1} (\det (L_{n,1}))^{\frac{1}{h}} \approx 9646700631 \). Lemma 1 shows for \( b_i \sim (u, v) \) and \( v \leq p_n \), \( \varepsilon = \frac{1}{4} \) that \( |u - vN| < p_n \|b_i - N_1\| 8/7 \leq p_n \|b_i\|/\sqrt{192} \leq 9340283.116 = 1153^2 \) for \( z = 2.276534496 \). Then \( |u - vN| \) is \( p_n \)-smooth with probability \( \rho(z) \approx \rho(2)(\frac{243}{224})^{0.276534496} \approx 0.132972 \) where \( 1/\rho(z) = 7.52 \).

3. Let \( b \sim (u, v) \) be the vector of \( L_{n,1} \) that yields the fac-relation in step 2. Eliminate some prime factor \( p_i \) of \( (u, v) \) from the prime basis and adjust the result of the primal-dual reduction to this change. Then a few iterations of algorithm 6.3.1 satisfy to complete the primal dual reduction for the prime basis without \( p_i \). Also adjust and of the independent trials of step 2 to this changed
prime basis. Continue to generate enough fac-relations for factoring $N$ this way. Then the number of arithmetic operations of step 3 should be negligible compared to step 2. Then $N \approx 2^{200}$ gets factored by $3.34 \cdot 10^{13}$ arithmetic operations.

$\#$(arithmetic steps for factoring $N \approx 2^{200}$): Perform the above step 2, for $n = 383, p_n = 2647$.

Primal-dual reduce the basis $R = [r_{i,j}]_{1 \leq i,j \leq 384}$ in $\mathbb{R}^{384 \times 384}$ by algorithm 6.3.1 (script), where $384 = bh, h = 384/k = 16$. Theorem 6.3.2 (script) shows that this yields a vector $b_1 \in \mathcal{L}'_{n,1}$ with $|b_1| = \sqrt{3} \frac{1}{\gamma_2} \frac{5}{12} (\det(\mathcal{L}_{n,1}))^{1/2} = 8.2221283186 \cdot 10^{11}$. Lemma 1 shows for $b_1 \sim (u, v)$ and $v \leq p_n, \varepsilon = \frac{1}{2}$ that

$$|u - vN| < p_n |b_1 - N|/(1-\varepsilon/2) \leq p_n \cdot |b_1|/\sqrt{834}/(1-\varepsilon/2) \leq 139982066.7 = 2647^z$$

for $z = 3.739976048$. Then $|u - vN|$ is $p_n$-smooth with probability $\rho(z) \approx \rho(2)(\varepsilon^{20})^{0.379976048} = 0.1529529184$ where $1/\rho(z) = 6.538$. Hence we get one fac-rel by 6.538 independent trials where before the primal-dual reduction each of the first 383 lines of $[r_{i,j}]_{1 \leq i,j \leq 384}$ is multiplied with probability $\frac{1}{2}$ by 2. This algorithm performs for each trial $\frac{n^2}{\frac{\sqrt{22}}{2}} \cdot \log_{1/2}(\alpha)$ iterations, each iteration HKZ-reduces two blocks $B_{i+1}, B_t \in \mathbb{R}^{x_4}$ using per block $k^{(3/8+1,1)}$ arithmetic steps, see (4.4).

Then one fac-rel is found by $\frac{\sqrt{22}}{2} \log_{1/2}(\alpha) k^{(3/8+1,1)} \approx 6 \cdot 10^{13}$ arithm. steps. This already includes the steps for step 3. and bounds the number of arithmetic operations for factoring $N \approx 2^{200}$.

**Factorisation time for QS and NFS:** QS uses for the factorisation of $N \approx 2^{200}$ that $p_n \approx e^{1/(\sqrt{\log N}{\log \log N})} \approx \frac{3.79 \cdot 10^{80}}{p_n}$, see [CP01, section 6.1]. The prime base for NFS is even bigger than for the quadratic sieve QS. The number of arithmetic steps of our factorisation is quite small compared with QS and NFS factorisation but the bit length of integers is large. The numbers of arithmetic steps for QS, NFS factorisation of $N \approx 2^{200}$ in [CP01, section 6.2]:

$$e^{\sqrt{\log N}{\log \log N}} \approx 1.415 \cdot 10^{17} \text{ for QS}$$

$$e^{(64/9)^{1/3}(\log N)^{1/3}(\log \log N)^{2/3}} \approx 1.675 \cdot 10^{17} \text{ for NFS}.$$ .

**NFS factoring of $N \approx 2^{200}$ performs $2.812 \times 10^{23}$ arithmetic steps.**

---

**New Enum for CVP of the prime number lattice creating fac-relations**

**INPUT:** $B, R = [r_{i,j}] \in \mathbb{R}^{n \times n}, B_{n,c}, c, T, \tau_i, \tau_n, A \in \mathbb{Q}$ such that $||L - N||^2 \leq A, s_{max}$.

**OUTPUT:** a sequence of $b = \sum_{i=1}^{n} u_i b_i \in \mathcal{L}$ where $|b - N_k|$ decreases to $|\mathcal{L} - N_k|$. $\tau_1, \tau_n, u_{n+1} = 0, s := 5$

1. $t := n, L := \emptyset, \gamma_n := [y_{n}], \gamma_{n+1} := 0, \nu = 5$

2. WHILE $t \leq n$ 

3. # perform stage $(t, u_1, ..., u_n, y_1, ..., y_t, y_{t+1})$:

   $$\left[ c_i = c_{i+1} + (u_i - y_i)^2 r_i^2 \right]$$

   IF $c_i \geq \tilde{A}$ THEN $GO$ TO 2.1 $\#$ this cuts the present stage

   $$\bar{y}_i := \bar{y}_{i-1} \frac{\gamma_2}{\gamma_1} \frac{\tilde{a}}{a_i} \tilde{a}$$

   IF $t = 1$ THEN $b := \sum_{i=1}^{n} u_i b_i, \tilde{A} := \tilde{c} = \frac{\gamma_t - \gamma_n}{\tau_t - \tau_n} \sum_{i=1}^{n} u_i y_i, s := \sum_{i=1}^{n} u_i y_i$ update all stored $\bar{y}_i, \tilde{A}$, the new $A$ $GO$ TO 2.1

4. IF $2^{s_{max}} < \tilde{A} < 2^{-s}$ THEN $[\text{store the stage and } \bar{y}_i, \bar{y}_i \in L, \bar{y}_i \in \mathbb{L}, \bar{y}_i \in 2.1

   [ t := t + 1, y_i := \tau_i, u_i := u_i, u_i := u_i + t_i y_i, y_i := y_i + 1 ]$

5. perform all stages $u_i := (u_1, ..., u_n, y_1, \nu := 1, \nu := 1, \nu := 1, \nu := 1)$

6. IF steps 2, 3 did not decrease $A$ for the current $s$ THEN terminate.

7. $s := s + 1$;

8. IF $s > s_{max}$ THEN restart with a larger $s_{max}$.

---

**Outline of the CVP-algorithm for $B_{n,c, N}$ using New Enum.** Let $B = QR = B_{n,c} T = [b_1, ..., b_n] \in \mathbb{Z}^{(n + 1) \times n}$ be a BKZ-basis of $\mathcal{L}(B_{n,c})$, $|\det(T)| = 1$. For $u = (u_1, ..., u_n) \in \mathbb{Z}^{n}$ we denote $u' = (u_1, ..., u_n)' = Tu$ so that $b := B_{n,c} u' = Bu \sim (u,v)$ where $u = \prod_{i=0}^{n} P_i^{u_i}, v = \prod_{i=0}^{n} P_i^{-u_i} \in \mathbb{N}$. We replace the input $N_c$ by its projection $\tau(N_{c}) = \sum_{i=1}^{n} \tau_i b_i \in \text{span} \mathcal{L}$, $13$
where $\tau : \mathbb{R}_{n+1} \to \text{span}(\mathcal{L})$ satisfies $\mathbf{N}_r - \tau(\mathbf{N}_r) \in \mathcal{L}^\perp$. Then $\tau(\mathbf{N}_r) = d\mathbf{B}_{n,v} \mathbf{1} = d\mathbf{B} \mathbf{T}^{-1} \mathbf{1}$ holds for $d := \ln N/(N - 2c + \sum_{i=1}^n \ln p_i)$, $1 := (1, \ldots, 1)^t \in \mathbb{Z}^n$.

Starting at $t = n$ the algorithm tries to satisfy (5.9) as $t$ decreases to 1.

$$
\|\pi_t(b - \tau(\mathbf{N}_r))\|^2 \leq \frac{n+1}{2c - 1} \ln N + \frac{n^2}{2c - 1} \ln(\mathbf{N}_r)
$$

for $b = \mathbf{Bu} \sim (u,v)$ (5.9)

This clearly holds for $t = n + 1$. If it holds at $t = 1$ then $\|b - \tau(\mathbf{N}_r)\|$ and $|u - v/N|$ are so small that they can provide a relation (5.1). We denote $\bar{c}_t = c_t(\tau_t - u_t, \ldots, \tau_t - u_t) = \|\pi_t(\tau(\mathbf{N}_r) - \mathbf{Bu})\|^2$.

Recall that $\bar{h}_t := V_{t-1} (\tilde{r}_1^{1/2}) (\tilde{r}_2^{1/2}) \cdots (\tilde{r}_{t-1}^{1/2})$ for $\tilde{h}_t := (A - \bar{c}_t)^{1/2}$ where $A \geq \|\mathcal{L} - \tau(\mathbf{N}_r)\|^2$. The success rate $\bar{h}_t$ increases as $\bar{c}_t$ decreases. The stored stages with small success rate $\bar{h}_t$ will be done at all stages with higher success rate $\bar{h}_t$. They can be cut off if $\bar{h}_t$ is extremely small or if to many stages with higher success rate $\bar{h}_t$ have been stored and the algorithm runs out of storage space. For the corresponding SVP-algorithm for $\mathcal{L}'$ we initially replace $\mathbf{B}_{n,v}$ by $[\mathbf{N}_r, \mathbf{B}_{n,v}]$.

Extending New Enum by continued fractions (CF). A. Schickelanz [S16] has extended New Enum by continued fractions generating fac-relations with large non $p_n$-smooth $v$. Take $b = \sum_{j=1}^n u_j \mathbf{b}_j \in \mathcal{L}(\mathbf{B}_{n,v})$ at stage $(1, u_1, \ldots, u_n)$ of New Enum and $(u, v) \sim b$, $u = \prod_{j \geq 0} p_j^{u_j}$ and compute the regular CF $\frac{\nu}{\psi}$ of $\delta := \frac{\nu}{\psi} - \frac{1}{\psi}$ with denominators $k_1 \leq p_n$. This starts with $\alpha_0 = [\delta], \alpha_1 = 1/\delta$ and iterates $\alpha_{i+1} := 1/(\alpha_i - \alpha_1)$ as long as $\alpha_i > \alpha_1$. Then $\frac{h_i}{k_i}$ is given by $h_i = [\alpha_i] h_{i-1} + h_{i-2}$ and $k_i = [\alpha_i] k_{i-1} + k_{i-2}$ where $h_{i-1}, h_{i-2}, k_0 = (1, 0, 0, 1)$ and $h_1 = 1$, $k_1 = [\alpha_1]$, hence $k_i \geq [\alpha_i]$. Each $\frac{h_i}{k_i}$ is a best approximation under all rational approximations $\frac{b}{k}$ of $[\delta]$ with denominators $k \leq k_i$. Lagrange has proved that $|\delta - \frac{b}{k}| \leq \frac{1}{\psi_{i+1}}$ and that equality holds if and only if $|\delta| = \frac{1}{\psi_{i+1}}$. This implies

Lemma 3. $|\pi_t - \pi_t N| \leq N/k_{i+1}$ holds for $\pi_t := u_k$ and $\pi_t := [\frac{\nu}{\psi}] k_i + \text{sign}(\delta)h_i$, where $|\pi_t - \pi_t N|$ yields a relation (5.1) if $k_i$ and $|\pi_t - \pi_t N|$ are $p_n$-smooth.

Proof. $|\pi_t - \pi_t N| = |(u - [\frac{\nu}{\psi}]N)k_i + \text{sign}(\delta)h_i, N| = |[(u - [\frac{\nu}{\psi}]N)k_i + \text{sign}(\delta)h_i, N]| \leq N/k_{i+1}$ since $|\delta| = \frac{1}{\psi_{i+1}}$ holds due to Lagrange’s inequality.

The fac-relations via CF have extremely large $\pi_t > N^2$. For $N \approx 10^{14}, n = 90, p_n = 463$ and $c = 1.4$ and one fixed scaling Schickelanz’s program found 14,000 fac-relations in 966 seconds, i.e., it took 0.067 seconds per relation and factored $N \approx 10^{14}$ in 6.8 seconds. See below the first 10 of the 14,000 relations. This performance of CF for $N \approx 10^{14}$ is due to $N < p_n^6$. But the fac-relations generated by CF vanish as $p_n^6/N$ decreases. We can increase the number of $p_n$-smooth $k_i$ by using $\alpha_{i+1} := 1/(\alpha_i - \beta_i)$ for many $\beta_i \in \mathbb{N}$ by $|\alpha_i - \beta_i| = O(1)$.

The first 10 of the 14,000 relations found for $N \approx 10^{14}$ via continued fractions for just one scaling

<table>
<thead>
<tr>
<th>$u$</th>
<th>$v$</th>
<th>$w$</th>
<th>$x$</th>
<th>$y$</th>
<th>$z$</th>
</tr>
</thead>
<tbody>
<tr>
<td>98</td>
<td>82</td>
<td>73</td>
<td>56</td>
<td>47</td>
<td>37</td>
</tr>
<tr>
<td>49</td>
<td>42</td>
<td>35</td>
<td>28</td>
<td>21</td>
<td>14</td>
</tr>
<tr>
<td>38</td>
<td>30</td>
<td>23</td>
<td>16</td>
<td>9</td>
<td>2</td>
</tr>
<tr>
<td>28</td>
<td>20</td>
<td>13</td>
<td>6</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>19</td>
<td>11</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
Extending this equation from $N$ to various integers $an$ with $p_n < a < p_n^2$. We can store $a$ with the stored stages. It can be useful to increase the success rate $\beta$ for $v = v'$ with a small $v'$ because this can simplify solving $v^p = \pm 1 \mod N$ and factoring $N$. This would be a step towards the quadratic sieve QS, see [CP01], section 6.1.

Comparison with [S93]. Our new results show an enormous progress compared to the previous approach of [S93]. [S93] reports on experiments for $N = 231438662079 \approx 2.1 \cdot 10^{12}$, $N_e = 10^{25}$, $c \approx 2.0278$ and the prime number basis of dimension $n = 125$ with diagonal entries $\ln p_i$ for $i = 1, ..., n$ instead of $\ln p_i$. The larger diagonal entries $\ln p_i$ require a larger $c$ and more time for the construction of relations (5.1). The latter took 10 hours per found relation on a PC of 1993.

6 Exponentially many fac-relations for large $v$

Now let $p_n = (\ln N)^n$ for a small $\alpha > 2$ and a large $N$. Then $p_n$ and $n$ are larger than for the factoring experiments reported in section 5. Theorem 2 shows for the larger $n$ that there are exponentially many $p_n$-smooth $u,v$ such that $|u-v| = 1$, $\frac{1}{4}N^\delta \leq v \leq N^\delta$. Theorem 3 shows under the assumptions of Theorem 2 and Prop. 1 that vectors $\tilde{b} \in \mathcal{L}(\mathcal{B}_{n,c})$ closest to $N_z$ can be found in pol. time.

The proof combines the results of Theorem 2, Prop. 1, Lemma 1, Lemma 2 and Cor. 3. We denote for $\delta > 0$

$$M_{N,n,\delta} = \left\{(u,v) \in \mathbb{N}^2 \mid |u-v| = 1, \frac{1}{4}N^\delta \leq v \leq N^\delta, u,v \text{ are } p_n\text{-smooth} \right\}.$$ 

Clearly every $(u,v) \in M_{N,n,\delta}$ yields a relation (5.2) because $|u-v| = 1$ and $u,v$ is $p_n$-smooth. Theorem 2 shows that $\#M_{N,n,\delta} \geq N^\varepsilon = 2^{5\delta}$, it is exponential in the bit length $k$ of $N$.

Theorem 2. Let $\alpha \geq 1.01 \frac{2^{k+1}}{\ln \ln \ln N}$ and $0 < \varepsilon < \delta < \alpha \ln \ln N$. Assume the events that $u$, resp. $v$ is $p_n$-smooth are nearly statistically independent for random $v$, $\frac{1}{2}N^\delta \leq v \leq N^\delta$ under the equation $|u-v| = 1$ then $\#M_{N,n,\delta} \geq N^\varepsilon$ holds for sufficiently large $N$.

Proof. (5.7) shows for $y^e = N, y = (\ln N)^n = p_n = N^{1/\varepsilon}, z = \ln N/\alpha \ln \ln N$ that

$$\Psi(N,p_n)/N = \left(\frac{e^{\varepsilon+1}}{\ln 2}\right)^z = z^{-z^{-o(z)}}$$

holds for $z \to \infty$. Extending this equation from $N$ to $N^\delta$ and $N^{1+\delta}$ our assumption shows for large $N$:

$$\#M_{N,n,\delta} \geq N^\delta(z^\delta)^{-z^\delta-o(1)}(z^\delta + z)^{-z^\delta-z^{-o(z)}},$$

ln $\#M_{N,n,\delta} \geq \delta \ln N - z^\delta \ln(z^\delta) - (z^\delta + z) \ln(z^\delta + z)(1 + o(1))$.

Here $N^\delta$ counts twice the number of integers $v$, $\frac{1}{2}N^\delta \leq v \leq N^\delta$. For every such $v$ there are two $u = v\pm 1$ and $(z^\delta)^{-z^\delta-o(1)}(z^\delta + z)^{-z^\delta-z^{-o(z)}}$ lower bound the portions of these $v$ and $u$ that are $p_n$-smooth. We assume that the $p_n$-smoothness events for $u$ and $v$ are nearly statistically independent of the equation $|u-v| = 1$. Hence we get for $z = \ln N/\alpha \ln \ln N$ that

$$\ln \#M_{N,n,\delta} \geq \delta \ln N - \frac{(z^\delta+1)\ln N\ln(z^\delta)}{\ln \ln N}(1 + o(1))$$

( since $\ln(z^\delta + z) = 

\ln(z^\delta)(1 + o(1))$ for large $z$ and constant $\delta$ )

\[\text{15}\]
\[ \alpha > \delta \ln N - \frac{(2k+1)}{\alpha} \ln (\ln N - \ln \alpha) + \ln \delta \] (since \( \alpha < \alpha \ln N \))

\[ \geq \ln N (\delta - \frac{(2k+1)}{\alpha} 1.01) \] (for large \( N \))

\[ > \varepsilon \ln N \] since \( \alpha > 1.01 \frac{2k+1}{\alpha} \).

Hence \( \# M_{N,n,\delta} \geq N^\varepsilon \). \hfill \Box

**Theorem 3.** Let \( 1 < c < (\ln N)^{n/2 - 1} \). Assume the events that \( u, v \) are \( p_u, p_v \)-smooth are nearly statistically independent for random \( u, v \), \( \frac{1}{2}N^c \leq v \leq N^c \) under the equation \( |u - v| = 1 \). Then \( \lambda_1^2 = 2c \ln N (1 + o(1)) \) for \( L := L(B_{n,c}) \) and \( N \to \infty \). We denote

\[ \tilde{M}_{N,n,c} = \{ (u, v) \in \mathbb{N}^2 \mid |u - v| = 1, \frac{1}{2}N^c \leq v \leq N^c \}. \]

Following the proof of Theorem 2 for \( c = 2 \) we see that \( \# \tilde{M}_{N,n,c} \geq N^c (z c)^{-2e-\alpha(z)} \) holds for

\[ z = \frac{1}{\ln \ln N}. \]

Recall that \( (u, v) \in \tilde{M}_{N,n,c} \) defines a vector \( b \sim (u, v) \) in \( L \). Hence

\[ \ln \# \tilde{M}_{N,n,c} \geq \ln N (c - \frac{2}{\alpha} (1 + o(1))) = \Theta(\ln N), \]

since \( \alpha > 2 \) and \( 1 < (\ln N)^{n/2 - 1} \). Let \( L(B_{n,c}) \ni b \sim (u, v) \in \tilde{M}_{N,n,c} \) and let \( u, v \) be essentially square-free except for a few small primes. We see from \( \frac{1}{2}N^c \leq v \leq N^c \) and \( u = v + 1 \) that

\[ \|b\|^2 = \ln u (1 + o(1)) + z_b^2 \leq 2c \ln N (1 + o(1)) + z_b^2, \]

where \( c \ln N - 1 \leq \ln v \leq c \ln N \). Moreover \( z_b^2 = N^{2c} \ln^2 (u/v) \) where \( \ln (u/v) = \ln (1 + \frac{z_b}{\sqrt{2}}) \leq \frac{1}{2} (1 + o(1)) \leq 2N^{-c} (1 + o(1)) \) holds for large \( N \). Hence \( z_b^2 \leq 4 (1 + o(1)) \) and thus \( \lambda_1^2 \leq 2c \ln N (1 + o(1)) \). On the other hand \( \lambda_1^2 \geq 2c \ln N \) holds by Lemma 2 and thus \( \|b\|^2 / \lambda_1^2 = 1 + o(1) \).

Next we bound \( rd(L) \) for \( L = L(B_{n,c}) \). Using \( \gamma_n \geq \frac{1}{\sqrt{\ln (n p_n) o(1)}} \cdot N^{2c/n} \), we get

\[ \gamma_n (\det L) \frac{1}{2} \geq \frac{1}{\sqrt{\ln (n p_n) o(1)}} \cdot N^{2c/n}, \]

and thus

\[ rd(L) = \lambda_1 / (\sqrt{\gamma_n (\det L) \frac{1}{2}}) = \left( \frac{2k+1}{\alpha} \ln N \right)^{1/2} / N^{c/n} (1 + o(1)). \]

Moreover \( c \leq (\ln N)^{n/2 - 1} = \sqrt{\ln N} / \ln N \) implies \( N^{c/n} = e^{\sqrt{c/n}} = e^{o(1)} \) and \( N^{c/n} = 1 + o(1) \). Hence

\[ rd(L) = (\ln N / p_n)^{1/2} (1 + o(1)) = O(\ln N)^{1/2} \]

\[ = O(p_n^{o(1)/2}) = O(p_n^{1/4}) = o(n^{-1/4}), \]

since \( p_n = O(n \ln n) \) and \( c = (\ln N)^{n/2 - 1} \) and \( \ln N = n^{1/2} \alpha > 2 \).

Following the proof of Prop. 1 and Cor. 3 NEW ENUM for CVP finds for \( p_n = (\ln N)^n \) some \( b \in L(B_{n,c}) \) that minimizes \( \|b - N_n\| \) in polynomial time, without proving correctness of the minimization. This proves the polynomial time bound. \hfill \Box

**References**


[S13] C.P. Schnorr, Factoring integers by CVP Algorithms. Proceedings Number Theory and Cryptography, LNCS 8260, Springer-Verlag, Nov. 2013, pp. 73–93, this is an early version of the most recent version in //www.mi.informatik.uni-frankfurt.de/ Publications 2013