1 Factoring algorithm

We start off by analysing CVP for the lattice and vector

$$\mathcal{L} = \begin{pmatrix} c_1 & 0 & \dots & 0 & 0 \\ 0 & c_2 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & c_{n-1} & 0 \\ B\log p_1 & B\log p_2 & \dots & B\log p_{n-1} & B\log p_n \end{pmatrix} \quad \mathbf{a} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ B\log N \end{pmatrix}$$

and assume that $c_i > 0$.

Suppose that $\mathbf{b}$ is the closest vector in $\mathcal{L}$ to $\mathbf{a}$, given by

$$\mathbf{b} = \begin{pmatrix} e_1 c_1 \\ e_2 c_2 \\ \vdots \\ e_{n-1} c_{n-1} \\ B\log \prod_{i=1}^{n} p_i^{e_i} \end{pmatrix}$$

In some sense B controls how big e_i gets. The bigger B gets the bigger e_i gets.

Suppose that $e_i \neq 0$ for all i. If any of them is zero we can just repeat this analysis with a smaller lattice probably.

By Minkowski's lattice point theorem, we have

$$B\log\left(\frac{\prod_{i=1}^{n} p_i^{e_i}}{N}\right)\prod_{i=1}^{n-1} e_i c_i \leq |\det \mathcal{L}| = B\log p_n \prod_{i=1}^{n-1} c_i$$

Let $\varepsilon = \prod_{i=1}^{n} p_i^{e_i} - N$, then we have

$$\log p_n \geq \left(1 + \frac{\varepsilon}{N}\right)\prod_{i=1}^{n-1} e_i + O\left(\frac{\varepsilon^2}{N^2}\right)$$

Which gives us

$$\varepsilon \lessapprox N\left(\frac{\log p_n}{\prod_{i=1}^{n-1} e_i} - 1\right)$$

and if we assume e_i is somewhat random in a small range we immediately see that $\varepsilon \approx O(N)$, which tells us we need roughtly $O\left(\frac{N}{\log N^n}\right)$ lattices to obtain a fac-relation, which is pretty trash.

//todo: approx e_i with B but honestly looks quite bad lol