Construction for $\mathbb{Z}_m^*$ where m - not a prime.

Suppose $m = \prod_{i=1}^{t} q_i^{e_i} \Rightarrow \left(\mathbb{Z}/m\mathbb{Z}\right)^* \simeq \prod_{i=1}^{t}\left(\mathbb{Z}/q_i^{e_i}\mathbb{Z}\right)^*$

$\varphi: \mathbb{Z}^u \to \mathbb{Z}_m^*$ $\quad (x_1,\dots,x_u) \mapsto \prod_{i=1}^{u} p_i^{x_i} \bmod m$. $\quad \mathcal{L} = \ker\varphi$

$\mathcal{L} = \{(x_1,\dots,x_u) \mid \prod_{i=1}^{u} p_i^{x_i} = 1 \pmod m\}$ ($\{p_i\}$ same definition)

Let us take $\beta_1,\dots,\beta_t$: $\langle\beta_i\rangle = \left(\mathbb{Z}/q_i^{e_i}\mathbb{Z}\right)^*$

$\prod_{j=1}^{u} p_j^{x_j} = 1 \bmod m \iff \prod_{j=1}^{u} p_j^{x_j} = 1 \bmod q_i^{e_i} \iff \sum_{j=1}^{u} x_j \log_{\beta_i} p_j = 0 \bmod \varphi(q_i^{e_i})$

Define $m_{ij} := \log_{\beta_i} p_{u-t+j} \bmod \varphi(q_i^{e_i})$, $M = (m_{ij})_{i=1,j=1}^{t,t}$

Assume $\exists M^{-1}$ in the ring $\mathbb{Z}_{\varphi(m)}$

Also define $y = (y_1,\dots,y_t)$ $y_i = \log_{\beta_i}\beta \bmod \varphi(q_i^{e_i})$ $\quad y = y(p)$ for any p in $\mathbb{Z}_{q_i^{e_i}}^*$.

and $g_p = y M^{-1} \bmod \varphi(m)$

$y_j = (g_p M)_j = \sum_{i=1}^{t} g_{p,u-t+i}\, m_{ij} \pmod{\varphi(m)}$

$\forall i$: $\prod_{j=1}^{t} p_{u-t+j}^{g_{p,u-t+j}} \bmod q_i^{e_i} = \prod_{j=1}^{t} \beta_i^{m_{ij} g_{p,u-t+j}} \bmod q_i^{e_i} =$

$= \beta_i^{\sum m_{ij} g_{p,u-t+j}} \bmod q_i^{e_i} = \beta_i^{y_i} \bmod q_i^{e_i} = p \bmod q_i^{e_i}$

Therefore,

$\forall i = \overline{1,u-t}$ $\quad b_i = (0,\dots,\underbrace{1}_{i\text{th}},0\dots,-g_{p_i,u-t+1},\dots,-g_{p_i,u}) \in \mathcal{L}$

(Because $\dfrac{p_i}{\prod_{j=1}^{t} p_{u-t+j}^{g_{p_i,u-t+j}}} = 1 \bmod q_\ell^{e_\ell}\ \forall \ell$)

Thm: $\begin{pmatrix} I_{u-t} & -G \\ O_t & \varphi(m) I_t \end{pmatrix}$ is a basis of $\mathcal{L}$.

where $G = \left(g_{p_i,u-t+j}\right)_{i,j=1}^{t}$

Г We already proved that $b_1,\dots b_{u-t}$ belong to $\mathcal{L}$

$\forall i$ $\quad p_{u-t+i}^{\varphi(m)} = 1 \bmod m \Rightarrow b_{u-t+i},\dots,b_u \in \mathcal{L}$ as well.

It is left to prove $b_1,\dots,b_u$ span the lattice.

Take arbitrary $u \in \mathcal{L}$ $\quad u = (u_1,\dots,u_u)$

$s = u - \sum_{i=1}^{u-t} u_i b_i = (0,\dots,0,s_{u-t+1},\dots,s_u) \in \mathcal{L}$

we need to show $s_{n-t+1} = 0 \bmod \varphi(m)$

$\prod_{i=1}^{t} p_{n-t+i}^{s_{n-t+i}} = 1 \bmod m \iff \prod_{i=1}^{t} p_{n-t+i}^{s_{n-t+i}} = 1 \bmod q_j^{e_j} \ \forall j \iff$

$\iff \forall j \quad \beta_j^{\sum s_{n-t+i} m_{ji}} = 1 \bmod q_j^{e_j} \iff \forall j \ \sum s_{n-t+i} m_{ji} = 0 \bmod \varphi(q_j^{e_j}) \iff$

$\iff \forall j \ M\bar{s} = 0 \bmod \varphi(q_j^{e_j}) \iff M\bar{s} = 0 \bmod \varphi(m) \iff$ (M invertible)

$\iff \bar{s} = 0 \bmod \varphi(m)$ QED ⌟