- In de Index calculus methode wordt wordt voor een voortbrenger $g \in \mathbb{F}_q^\times$ en een element h het discrete logaritme $L(h)$ bepaald zdd $g^{L(h)} \equiv h \pmod{P}$
  In het eerste stap van dit algoritme wordt een factor base bepaald.
  Mijn vraag is nu: hoe bepaalt men in een implementatie van dit algoritme hoe groot deze factor base moet zijn?

- In het artikel wordt vermeld dat $E(\mathbb{F}_q) \cong C_{n_1} \bigoplus C_{n_2}$ waar C_n staat voor de cyclische group met n elementen en waarvoor geldt dat $n_2 \mid n_1$ en $n_2 \mid q-1$.
  Het is mij reeds gelukt om te bewijzen dat $E(\mathbb{F}_q) \cong C_{n_1} \bigoplus C_{n_2}$ met $n_2 \mid n_1$. Echter ik kan niet bewijzen dat $n_2 \mid q-1$.

- Ik het bestudeerde artikel wordt voor het bewijs van lemma 3 verwezen naar een artikel van Rene Schoof. Het lemma is de volgende:
  Lemma: Laat E een elliptische kromme zijn over $\mathbb{F}_q$ waar $q = p^k$ en laat t de trace zijn van het Frobenius Morphisme ϕ van E. Laat verder nog n een natuurlijk getal zijn zdd $ggd(p,n) = 1$. Dan zijn de volgende equivalent:

  1. $E(\bar{\mathbb{F}}_q)[n] \subseteq E(\mathbb{F}_q)$.
  2. $n^2 \mid q+1-t$, $n \mid q-1$ en ($\phi \in \mathbb{Z}$ of $\mathcal{O}(\frac{t^2-4q}{n^2}) \subseteq End_{\mathbb{F}_q}(E)$).
     (Met $\mathcal{O}(\frac{t^2-4q}{n^2})$ bedoeld men de complex quadratic order met discriminant $\frac{t^2-4q}{n^2}$)
     In het bewijs wordt gebruikt dat er een kanonieke injectieve afbeelding $End_{\mathbb{F}_q}(E)/nEnd_{\mathbb{F}_q}(E) \to End(E(\bar{\mathbb{F}}_q)[n])$ is. Ik heb twee vragen over dit lemma en het bewijs:
     - volgens het artikel van Rene Schoof wordt een complex quadratic order van een gegeven 'quadratic number field' uniek gekarakteriseerd door zijn discriminant. Echter wat is in ons geval dit 'quadratic number field'? Er wordt hier immers niks gezegd over of E supersingular is of niet, dus zijn endomorphisme ring hoeft niet perse een order in een 'quadratic number field' te zijn.
     - In het bewijs wordt in 1 regel gezegd dat (1) equivalent is met

       $$\frac{\phi - 1}{n} \in End_{\mathbb{F}_q}(E).$$

       Het is mij duidelijk dat (1) equivalent is met $E[n] \subseteq ker(\phi - 1)$ en het is gemakkelijk te bewijzen dat

       $$E[n] \subseteq ker(\phi - 1) \Rightarrow \frac{\phi - 1}{n} \in End_{\mathbb{F}_q}(E)$$

       Het lukt mij echter niet om de andere kant op te bewijzen.