Finding orders with prescribed index
Project Log

Alex J. Best

December 18, 2013

13/10/13

Implementations exist in Magma (refs) Finding power basis for order with specified index in a given order. 15/10/13

István Gaál has done a lot of work in this area, and there exists(ed) an implementation within KANT (run by Pohst). 16/10/13

Should think up naive algorithm first in a general setting (no power basis etc). Take an absolute number field $K|\mathbb{Q}$ and consider $\mathcal{O} \subset \mathcal{O}_K$ letting $I = [\mathcal{O}_K : \mathcal{O}]$ we should find a relation between I and the conductor of $\mathcal{O}$. Recall the conductor $\mathfrak{f}$ of $\mathcal{O}$ is the largest ideal of $\mathcal{O}_K$ contained in $\mathcal{O}$, so $\mathfrak{f} = \{\alpha \in \mathcal{O}_K \mid \alpha\mathcal{O}_K \subseteq \mathcal{O}\}$. Will probably come down to computing some quotient $\mathcal{O}/\mathcal{N}$. 25/10/13

We have that $\mathcal{O}_K/\mathcal{O} \cong (\mathcal{O}_K/\mathfrak{f})/(\mathcal{O}/\mathfrak{f})$ so we can see $[\mathcal{O}_K : \mathcal{O}][\mathcal{O} : \mathfrak{f}] = [\mathcal{O}_K : \mathfrak{f}]$. As we know the index we wish to obtain we know that the norm of the conductor of the order we are looking for is divisible by the index. This gives us some prime ideals that must divide the conductor so we start with these. We then calculate the possible conductors and their corresponding orders (how?). 7/11/13

Given $[F : \mathbb{Q}] = d$ we have $\mathcal{O}_F \subset F$ and $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_F$. Then $\mathcal{O}_F/\mathcal{O} = \mathcal{O}_F/f\mathcal{O}_f$ torsion module. $\text{norm}(f\mathcal{O}_F) = f^2 \in \mathbb{Z}$.

Can work one prime at a time (locally) then path things together for a speedup.