where n is a product of two primes). [The task denoted by "Pol. fact." means factoring polynomials in one variable over the residue class ring $\mathbb{Z}/n\mathbb{Z}$. We wont treat it in these lecture notes.]

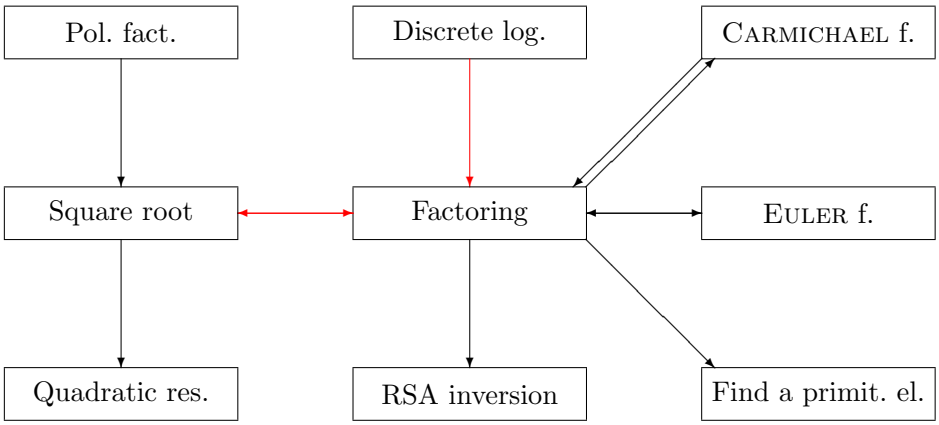

Figure 5.1: Connection between computational problems for a composite module