High Performance Computing - List 3

Deadline for the list: your laboratory classes between 19.03.2018 and 25.03.2018.

Task 1 (10 pts) In C/C++ implement the parallel version of the Pollard-ρ method for calculating discrete logarithms in finite groups. Use OpenMP. For big integers use NTL library. As an instance choose p being 40-60 bit number, random $g \in \mathbb{F}_p \setminus \{0\}$ such that ord$g$ is prime, and $y \in \langle g \rangle$ (hint: a strong prime is the least troublesome choice of p, for such a prime it is easy to choose g of prime order – consider the trick from the lecture).