High Performance Computing - List 1

Time for solving the list: two weeks.

Task 1 (5 pts) In C/C++ implement Pollard-ρ method for calculating discrete logarithms in finite groups. For big integers use NTL library. As an instance choose multiplicative group of prime field $\mathbb{F}_p$ for p being 40-60 bit number (hint: a strong prime is the least troublesome choice of p).