High Performance Computing - List 5

Deadline for the list: your laboratory classes between 07.05.2018 and 13.05.2018.

Task 1 (30 pts) In C/C++ implement the parallel version of the Pohlig-Hellman algorithm. Use OpenMP. For big integers use NTL library. As an instance choose prime modulus p such that:

$$p - 1 = 2^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k} \cdot Q, \tag{1}$$

where each p_i is a prime number having 40-50 bits in length, $k \in \{8, \dots, 12\}$, each α_i equals at least 3, and Q has no prime factors shorter than 256 bits.

Choose random $g \in \mathbb{F}_p^*$, random $x \in \{1, 2, \dots, k-1\}$, set $y = g^x \bmod p$, and with the Pohlig-Hellman algorithm calculate

$$x \bmod 2^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$$

on the basis of g, y, p only. Assume that you know the representation (1) of the number $p - 1$.