High Performance Computing - List 6

Deadline for the list: your laboratory classes between 04.06.2018 and 10.06.2018.

Task 1 (5 pts) Express $\mathbb{Z}^{\star}_{2584}$ as a cartesian product of cyclic groups of orders being powers of primes. On paper calculate the value of the number r being the greatest possible order of an element from $\mathbb{Z}^{\star}_{2584}$. Implement a test checking that for each $a \in \mathbb{Z}^{\star}_{2584}$ we have $a^r \equiv 1 \bmod 2584$.

Task 2 (25 pts) In C/C++ implement the parallel version of the ECM Algorithm. Use OpenMP. As an instance choose n being a product of two 75-80 bit primes. As scalar k take $B_1!$ for $B_1 = 10^5$ (you may experiment with greater B_1 or/and greater n). For $P \in E(\mathbb{Z}_n)$ calculate $k \cdot P$ as

$$B_1 \cdot ((B_1 - 1) \cdot (\cdots \cdot (2 \cdot P) \ldots)).$$

That is do not calculate $B_1!$ separately.