Jarosław Wróblewski (jwr@math.uni.wroc.pl), ESLP Problem Set

# Lesson 1 - Appendix A

If you decide to go through programming projects 7-9, you may consider the following change. This change may improve the program (and save memory), but it goes in the wrong direction if one wants to go to higher powers later.

You were supposed to put all $x < N$ in table 2 with $p$ **rows** in such a way that $r$-th row contains all numbers $x$ with $x^4 \equiv r \pmod{p}$.

Instead you may create a table with $(p-1)/2$ **entries** numbered 1 throuhg $(p-1)/2$. Then run through all $x$ from 1 to $(p-1)/2$ and put $x$ in position number

$$x^4 \pmod{p}$$

if

$$\left(x^4 \pmod{p}\right) < p/2\,.$$

If

$$\left(x^4 \pmod{p}\right) > p/2$$

put $-x$ in position number

$$p - \left(x^4 \pmod{p}\right)\,.$$

If you called the table $t$ then we will refer later to it's $r$-th entry as $t[r]$.

When later in the program you want to get the list of all $y$'s such that for given $r$ we have $y^4 \equiv r \pmod{p}$, then you do the following:

If $r = 0$ then $y$ must run through multiples of $p$.

If $r < p/2$ and $t[r] > 0$ then run through all $y$ with $y \equiv \pm t[r] \pmod{p}$.

If $r < p/2$ and $t[r] < 0$ then there are no $y$'s.

If $r > p/2$ and $t[p-r] > 0$ then there are no $y$'s.

If $r > p/2$ and $t[p-r] < 0$ then run through all $y$ with $y \equiv \pm t[p-r] \pmod{p}$.

**Remember** that $p$ **must** be of the form $4k+3$.

If for some reason you want to construct (3,2,2) or (5,2,2) searcher that way, take $p$ **not** of the form $6k+1$ (respectively $10k+1$). Then table described above should have $p$ entries as extracting 3rd (respectively 5th) root mod $p$ is unique in this case.