

4. Довести, что \sqrt{p} — простое
число, порождающее элемент

лемма $(\mathbb{Z}/p\mathbb{Z})^\times$ обратный 1.

Для $p=2$, все очевидно, малы в качестве $p > 3$.
 $\forall g$ точно G группа, но

$$\forall g \in G: \langle g \rangle = G \Rightarrow \langle g^{-1} \rangle = G$$

точно $\langle g \rangle = G$, а не при

$$\text{уборку } g = g^{-1}, \text{ но } g^2 = e$$

$$\Rightarrow |G| = 2.$$

Так же при $p > 3$, $|(\mathbb{Z}/p\mathbb{Z})^\times| =$

$$= p-1 > 2, \text{ но } \forall g \in (\mathbb{Z}/p\mathbb{Z})^\times:$$

$$\langle g \rangle = (\mathbb{Z}/p\mathbb{Z})^\times \Rightarrow g \neq g^{-1} \langle g^{-1} \rangle = (\mathbb{Z}/p\mathbb{Z})^\times.$$

Поэтому при $p > 3$ все порождают элементы $\mathbb{Z}/p\mathbb{Z}$ разбиваются на пары обратных, а малы их количество $p-1$.