1. (Е.И.Золотарев) Пусть p и q – различные нечетные простые числа. Рассмотрим множества $S = \{0, 1, \ldots, pq-1\}$ и $T = \{(a, b) | 0 \leqslant a < p, 0 \leqslant b < q\}$. Согласно китайской теореме об остатках отображение $c \mapsto (c \bmod p, c \bmod q)$ задает взаимно-однозначное соответствие между S и T.

а) Найдите четность подстановки множества T, переводящей (a, b) в $(a+pb \bmod p, a+pb \bmod q)$, и подстановки, переводящей (a, b) в $(qa + b \bmod p, qa + b \bmod q)$.

б) Найдите четность подстановки множества S, переводящей $a + pb$ в $qa + b$.

в) Выведите из пунктов а) и б) квадратичный закон взаимности.

2. Дано натуральное k.

а) Докажите, что для бесконечно многих натуральных n наибольший общий делитель чисел n и $[n\sqrt{k^2+1}]$ больше $0,1\sqrt{n}$.

б) Найдите наименьшее действительное α такое, что при всех натуральных n верно неравенство

$$(n, [n\sqrt{k^2+1}]) \leqslant \alpha\sqrt{n}.$$

3. (Критерий Люка-Лемера). Пусть $(1+\sqrt{3})^n = u_n + v_n\sqrt{3}$ с целыми u_m и v_n, $\beta = 1-\sqrt{3}$.

а) Определим *ранг* простого числа p как наименьший индекс ω, для которого v_w делится на p (если, конечно, такие индексы существуют). Докажите, что если ω – ранг простого p, то v_k делится на p тогда и только тогда, когда k делится на ω.

б) Докажите, что для любого простого p его ранг $\omega \leqslant p+1$.

в) Рассмотрим последовательность $\{s_k\}$: $s_1 = 4$, $s_2 = 14$, $\ldots$, $s_k = s_{k-1}^2 - 2$, $\ldots$. Докажите, что $u_{2^k} = 2^{2^{k-1}-1}s_k$.

г) Докажите, что если число Мерсенна $M_p = 2^p - 1$ простое, то s_{p-1} делится на M_p.

д) Докажите, что если s_{p-1} делится на M_p, то M_p простое.

4. Пусть p, q – простые числа, $q > 5$. Докажите, что если $q | 2^p + 3^p$, то $q > p$.

5. Докажите, что не существует натурального числа $n > 1$, для которого n делит $2^n - 1$.