# Примитивный вычет (*группа «11-Ь»*)

1. Найдите хотя бы один примитивный вычет по модулю 13.
2. Можно ли расставить по кругу числа 1, 2, ..., 12 так, чтобы для любых трех подряд идущих $a, b, c$ выполнялось $b^2 - ac \,\vdots\, 13$?
3. Докажите, что $a$ является примитивным вычетом по модулю простого $p \neq 2$ в том и только в том случае, если для любого простого $q$, делящего $p-1$, выполняется $a^{\frac{p-1}{q}} \not\equiv_p 1$.
4. Докажите, что если $(m, k) = 1$, то $\varphi(mk) = \varphi(m)\varphi(k)$.
5. Можно ли заполнить квадрат $4 \times 4$ числами 1, 2, ..., 16 (каждое использовать ровно один раз) так, чтобы произведения чисел по строкам и произведения чисел по столбцам (всего 8 произведений) давали равные остатки от деления на 17?
6. Пусть $p$ — простое число. Примитивным вычетом по модулю $p^2$ называется остаток $a$, степени которого $a, a^2, a^3, ..., a^k, ...$ при делении на $p^2$ дают все возможные остатки, *взаимно-простые* с $p$ (сколько таких остатков?). Докажите, что примитивный вычет по модулю $p^2$ существует.

**Примитивный вычет** (*группа «11-Ь»*)

1. Найдите хотя бы один примитивный вычет по модулю 13.

2. Можно ли расставить по кругу числа 1, 2, ..., 12 так, чтобы для любых трех подряд идущих $a, b, c$ выполнялось $b^2 - ac \,\vdots\, 13$?

3. Докажите, что $a$ является примитивным вычетом по модулю простого $p \neq 2$ в том и только в том случае, если для любого простого $q$, делящего $p-1$, выполняется $a^{\frac{p-1}{q}} \not\equiv_p 1$.

4. Докажите, что если $(m, k) = 1$, то $\varphi(mk) = \varphi(m)\varphi(k)$.

5. Можно ли заполнить квадрат $4\times 4$ числами 1, 2, ..., 16 (каждое использовать ровно один раз) так, чтобы произведения чисел по строкам и произведения чисел по столбцам (всего 8 произведений) давали равные остатки от деления на 17?

6. Пусть $p$ — простое число. Примитивным вычетом по модулю $p^2$ называется остаток $a$, степени которого $a, a^2, a^3, ..., a^k, ...$ при делении на $p^2$ дают все возможные остатки, *взаимно-простые* с $p$ (сколько таких остатков?). Докажите, что примитивный вычет по модулю $p^2$ существует.