Примитивные вычеты, квадратичные вычеты

1. Можно ли записать по кругу числа 1, 2, ..., 12 так, чтобы для любых трех подряд стоящих чисел a, b, c число $b^2 - ac$ делилось на 13?
2. Запишите в таблицу 4×4 числа 1,2, ..., 16 так, чтобы всевозможные произведения всех чисел, стоящих в одной строке, и всевозможные произведения чисел, стоящих в одном столбце, (т.е. всего 8 чисел) давали один и тот же остаток при делении на 17.
3. Пусть g —- первообразный корень по модулю m. При каких ℓ вычет g^l также будет первообразным корнем по модулю m?
4. * Пусть g —- первообразный корень по модулю $p \in \mathbb{P}$.
   а) Докажите, что найдётся t такое, что $(g+pt)^{p-1} = 1 + pu$, где u не делится на p.
   б) Докажите, что $\forall k \in \mathbb{N} \quad (g+pt)^{p^{k-1}(p-1)} = 1 + p^k u_k$, где u_k не делится на p.
   в) Докажите, что $\forall m \in \mathbb{N} \quad g+pt$ является первообразным корнем по модулю p^m.
5. Вычет a, для которого в $\mathbb{F}_p$ разрешимо уравнение $x^k = a$, называется k–степенным. Сколько существует таких вычетов для данного p?
6. * Пусть $p \in \mathbb{P}$, $p > 2$, $(a,p) = 1$, $p' = \dfrac{p-1}{2}$.
   Положим $1 \cdot a = \varepsilon_1 r_1$, $2 \cdot a = \varepsilon_2 r_2$, $\ldots, p' \cdot a = \varepsilon_{p'} r_{p'}$, где $\varepsilon_i = \pm 1$ и $r_i \in \{1, 2, ..., p'\}$.
   а) Все вычеты $r_1, r_2, ..., r_{p'}$ различны.
   б) $\left(\dfrac{a}{p}\right) = \varepsilon_1 \varepsilon_2 \ldots \varepsilon_{p'}$.
   в) $\left(\dfrac{a}{p}\right) = (-1)^{\sum_{k=1}^{p'} \left\lfloor \frac{2ak}{p} \right\rfloor}$.
7. * Пусть $p \in \mathbb{P}$, $p > 2$, $a \perp p$, $a \not\vdots 2$.
   а) $\left(\dfrac{2a}{p}\right) = (-1)^{\sum_{k=1}^{p'} \left\lfloor \frac{ak}{p} \right\rfloor + \frac{p^2-1}{8}}$;
   б) $\left(\dfrac{a}{p}\right) = (-1)^{\sum_{k=1}^{p'} \left\lfloor \frac{ak}{p} \right\rfloor}$.
   в) $\displaystyle\sum_{k=1}^{r'} \left\lfloor \frac{kq}{r} \right\rfloor + \sum_{k=1}^{q'} \left\lfloor \frac{kr}{q} \right\rfloor = \frac{r-1}{2} \cdot \frac{q-1}{2}$.
8. Является ли 1707 квадратичным вычетом по модулю 1777?
   (Почему именно 1707 и 1777?)

Примитивные вычеты, квадратичные вычеты

1. Можно ли записать по кругу числа 1, 2, ..., 12 так, чтобы для любых трех подряд стоящих чисел a, b, c число $b^2 - ac$ делилось на 13?
2. Запишите в таблицу 4×4 числа 1,2, ..., 16 так, чтобы всевозможные произведения всех чисел, стоящих в одной строке, и всевозможные произведения чисел, стоящих в одном столбце, (т.е. всего 8 чисел) давали один и тот же остаток при делении на 17.
3. Пусть g —- первообразный корень по модулю m. При каких ℓ вычет g^l также будет первообразным корнем по модулю m?
4. * Пусть g —- первообразный корень по модулю $p \in \mathbb{P}$.
   а) Докажите, что найдётся t такое, что $(g+pt)^{p-1} = 1 + pu$, где u не делится на p.
   б) Докажите, что $\forall k \in \mathbb{N} \quad (g+pt)^{p^{k-1}(p-1)} = 1 + p^k u_k$, где u_k не делится на p.
   в) Докажите, что $\forall m \in \mathbb{N} \quad g+pt$ является первообразным корнем по модулю p^m.
5. Вычет a, для которого в $\mathbb{F}_p$ разрешимо уравнение $x^k = a$, называется k–степенным. Сколько существует таких вычетов для данного p?
6. * Пусть $p \in \mathbb{P}$, $p > 2$, $(a,p) = 1$, $p' = \dfrac{p-1}{2}$.
   Положим $1 \cdot a = \varepsilon_1 r_1$, $2 \cdot a = \varepsilon_2 r_2$, $\ldots, p' \cdot a = \varepsilon_{p'} r_{p'}$, где $\varepsilon_i = \pm 1$ и $r_i \in \{1, 2, ..., p'\}$.
   а) Все вычеты $r_1, r_2, ..., r_{p'}$ различны.
   б) $\left(\dfrac{a}{p}\right) = \varepsilon_1 \varepsilon_2 \ldots \varepsilon_{p'}$.
   в) $\left(\dfrac{a}{p}\right) = (-1)^{\sum_{k=1}^{p'} \left\lfloor \frac{2ak}{p} \right\rfloor}$.
7. * Пусть $p \in \mathbb{P}$, $p > 2$, $a \perp p$, $a \not\vdots 2$.
   а) $\left(\dfrac{2a}{p}\right) = (-1)^{\sum_{k=1}^{p'} \left\lfloor \frac{ak}{p} \right\rfloor + \frac{p^2-1}{8}}$;
   б) $\left(\dfrac{a}{p}\right) = (-1)^{\sum_{k=1}^{p'} \left\lfloor \frac{ak}{p} \right\rfloor}$.
   в) $\displaystyle\sum_{k=1}^{r'} \left\lfloor \frac{kq}{r} \right\rfloor + \sum_{k=1}^{q'} \left\lfloor \frac{kr}{q} \right\rfloor = \frac{r-1}{2} \cdot \frac{q-1}{2}$.
8. Является ли 1707 квадратичным вычетом по модулю 1777?
   (Почему именно 1707 и 1777?)