Арифметика вычетов по модулю

Примитивные вычеты

1. Порядок степени вычета: Пусть $\mathrm{ord}_n(a) = d$. Тогда $\mathrm{ord}_n(a^k) = \dfrac{d}{(d,k)}$.

2. Примитивный вычет: $(\mathbb{Z}/n\mathbb{Z})^\times = < g >$, т.е. $\mathrm{ord}_n(g) = \varphi(n)$.
   Он же *первообразный корень*.

3. По модулю $p \in \mathbb{P}$ примитивный вычет существует.
   □ Пусть $\psi(d) = |\{a \in (\mathbb{F}_p)^\times : \mathrm{ord}_p(a) = d\}|$ — количество вычетов порядка d.
   Первое. $\sum\limits_{d|p-1} \psi(d) = p-1$. Ранее мы видели, что $\sum\limits_{d|p-1} \varphi(d) = p-1$.
   Второе. Если a такой, что $\mathrm{ord}_p(a) = d$, то все корни $x^d - 1 = 0$ в списке $1, a, a^2, \ldots, a^{d-1}$.
   Третье. $\forall d|p-1\ \psi(d) \in \{0; \varphi(d)\}$.
   Четвёртое. $\forall d|p-1\ \psi(d) = \varphi(d)$. ■

4. Примитивные вычеты существуют в точности по модулям 2, 4, p^γ и $2p^\gamma$ (где $p \in \mathbb{P}$, $p > 2$, $\gamma \in \mathbb{N}$).

Квадратичные вычеты ($p \in \mathbb{P}$, $p > 2$)

5. Квадратичный вычет: $a \equiv_p b^2$ для некоторого b
   невычет: $a \not\equiv_p b^2$ для всех b

   Символ Лежандра $\left(\dfrac{a}{p}\right) = \begin{cases} 0, & a \text{ кратно } p \\ +1, & a \text{ — квадратичный вычет, не кратный } p \\ -1, & a \text{ — квадратичный невычет} \end{cases}$

   Критерий Эйлера: $\left(\dfrac{a}{p}\right) \equiv_p a^{\frac{p-1}{2}}$

   □ Многочлен $x^{\frac{p-1}{2}} - 1 = 0$ имеет не более deg корней. ■

   Свойство символа Лежандра: $\left(\dfrac{bc}{p}\right) = \left(\dfrac{b}{p}\right)\left(\dfrac{c}{p}\right)$.

6. $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

7. Квадратичный закон взаимности: $r, q \in \mathbb{P}\backslash\{2\},\ r \neq q \Rightarrow \left(\dfrac{q}{r}\right) \cdot \left(\dfrac{r}{q}\right) = (-1)^{\frac{r-1}{2} \cdot \frac{q-1}{2}}$.