Составной модуль

Определение: число a, называется квадратичным вычетом по модулю m, если оно взаимно просто с ним и существует такое число z, что $z^2 \equiv a \pmod{m}$.
Во всех задачах листка p — нечётное простое число.

1. Известно, что $(a, b) = 1$. Докажите, что число c является квадратичным вычетом по модулю ab тогда и только тогда. когда оно является квадратичным вычетом по модулям a и b.

2. а) Докажите, что по модулю p^α ровно половина взаимно простых с модулем вычетов будут являться квадратичными. б) Докажите, что по модулю p^α вычет является квадратичным тогда и только тогда, когда он является квадратичным по модулю p.

3. а) Докажите, что если вычет a является квадратичным по модулю 2^α, то $a \equiv 1 \pmod{8}$. б) Докажите, что по модулю 2^α существуют ровно $2^{\alpha-3}$ квадратичных вычетов. в) Докажите, что квадратичными вычетами по модулю 2^α будут являться те и только те вычеты, которые при делении на 8 дают остаток 1.

4. Докажите, что если $m = 2^\alpha \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, то количество квадратичных вычетов по этому модулю равно $Q(m) = \dfrac{\varphi(m)}{2^k q(m)}$; где $q(m)$ — это 1 при $\alpha \leqslant 1$, 2 при $\alpha = 2$, и 4 при других значениях α.

Определение: Символом Якоби $\left(\dfrac{a}{n}\right)$ называется произведение символов Лежандра вида $\left(\dfrac{a}{p_k}\right)$, если $n = p_1 \cdot p_2 \cdot \ldots \cdot p_m$)

5. Докажите свойства символа Якоби:
а) $\left(\dfrac{ab}{n}\right) = \left(\dfrac{a}{n}\right) \cdot \left(\dfrac{b}{n}\right)$; б) $\left(\dfrac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$; в) $\left(\dfrac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$

6. а) Докажите, что если символ Якоби равен минус одному, то число a — квадратичный невычет по модулю n. б) Приведите пример, когда символ Якоби равен одному, но a — квадратичный невычет по модулю n.

7. Докажите для взаимно простых нечётных m и n квадратичных закон взаимности для символов Якоби:

$$\left(\frac{m}{n}\right) \cdot \left(\frac{n}{m}\right) = (-1)^{\frac{(m-1)(n-1)}{4}}$$