Первообразный корень

Первообразный корень = примитивный вычет

1. Докажите, что c является первообразным корнем по модулю простого $p \neq 2$ в том случае, если для любого простого q , делящего $p - 1$, выполняется $c^{\frac{p-1}{q}} \not\equiv 1(p)$.
2. Пусть c — первообразный корень для простого p . Докажите, что c^k является первообразным корнем в том и только том случае, если $(k, p - 1) = 1$.
3. Найдите первообразный корень по модулю (a) 23 (b) 257
4. Пусть m делится на различные простые числа p_1 и p_2 ; $(a, m) = 1$.
 - а) Докажите, что $a^{\frac{\phi(m)}{2}} \equiv 1(m)$. (Указание: укажите все числа вида a^k , которые делятся на p_1 ; вспомните формулу для $\phi(m)$.)
 - б) Докажите, что в мультипликативной группе по модулю m нет первообразного корня.
5. Докажите, что $5^{2^k} \equiv 2^{k+2} + 1 \pmod{2^{k+3}}$. (Указание: воспользуйтесь математической индукцией.)
6. Докажите, что 2 является первообразным корнем по модулю 5^n .

Первообразный корень

Первообразный корень = примитивный вычет

1. Докажите, что c является первообразным корнем по модулю простого $p \neq 2$ в том случае, если для любого простого q , делящего $p - 1$, выполняется $c^{\frac{p-1}{q}} \not\equiv 1(p)$.
2. Пусть c — первообразный корень для простого p . Докажите, что c^k является первообразным корнем в том и только том случае, если $(k, p - 1) = 1$.
3. Найдите первообразный корень по модулю (a) 23 (b) 257
4. Пусть m делится на различные простые числа p_1 и p_2 ; $(a, m) = 1$.
 - а) Докажите, что $a^{\frac{\phi(m)}{2}} \equiv 1(m)$. (Указание: укажите все числа вида a^k , которые делятся на p_1 ; вспомните формулу для $\phi(m)$.)
 - б) Докажите, что в мультипликативной группе по модулю m нет первообразного корня.
5. Докажите, что $5^{2^k} \equiv 2^{k+2} + 1 \pmod{2^{k+3}}$. (Указание: воспользуйтесь математической индукцией.)
6. Докажите, что 2 является первообразным корнем по модулю 5^n .