Первообразные корни

Определение 1: вычет g называется первообразным корнем по модулю m, если его показатель по модулю m равен $\varphi(m)$.
Определение 2: вычет g называется первообразным по модулю m, если все взаимно простые с m вычеты являются степенями g.

1. а) Докажите, что если по модулю m есть первообразный корень, то квадратичных вычетов по этому модулю ровно $\frac{\varphi(m)}{2}$.
б) Докажите, что если по модулю m есть первообразный корень, то количество первообразных корней равно $\varphi(\varphi(m))$.

2. Докажите, что первообразного корня не существует по модулям вида pq, $4p$, 2^m ($m \geqslant 3$), при простых нечётных p и q.

3. (*существование первообразного корня по простому модулю*) а) В строку выписали все правильные дроби со знаменателем n и единицу: $\frac{1}{n}$, $\frac{2}{n} \ldots \frac{n-1}{n}$, $\frac{n}{n}$. После этого каждую дробь сократили на НОД числителя и знаменателя. Сколько получилось дробей со знаменателем d, где d — произвольный делитель числа n?
б) Выведите из этого *тождество Гаусса*: $\sum\limits_{d|n} \varphi(d) = n$.

в) Рассмотрите многочлен $x^d - 1$ по модулю p и по индукции получите, что показателю d по модулю p принадлежат ровно $\varphi(d)$ вычетов, если $d|n$, где $n = \varphi(p)$.

4. Понятно каким способом докажите, что сравнение $x^3 \equiv a \pmod p$ при $p = 3k + 2$ имеет единственное решение, а при $p = 3k + 1$ имеет либо 0 решений, либо 3.

5. Докажите, что из сравнений $x^3 \equiv a \pmod p$, $x^3 \equiv b \pmod p$, $x^3 \equiv c \pmod p$, $x^3 \equiv ab \pmod p$, $x^3 \equiv ac \pmod p$, $x^3 \equiv abc \pmod p$ хотя бы одно имеет решение.

6. Пусть g — первообразный корень по модулю p. а) Докажите, что либо g, либо $g + p$ являются первообразным корнем по модулю $2p$; б) Докажите, что по модулю p^2 существует первообразный корень, который сравним с g по модулю p.

7. а) Докажите, что первообразный корень по модулю p^2 является первообразным корнем по модулю p^α при всех натуральных α; б) Докажите, что по модулю $2p^\alpha$ также существует первообразный корень.

8. Докажите, что число 2 является первообразным корнем по модулю а) 3^m; б) 5^m.