Многочлены над конечным полем и ТЧ

Во всём листике p — простое число.

1. а) Докажите, что для любого $m \not\vdots p-1$ существует такое n, что $(n,p)=1$, $n^m \not\equiv_p 1$.

б) Пусть m — натуральное число. Рассмотрим сумму

$$S=\sum_{x\in\mathbb{Z}_p} x^m.$$

Тогда либо $S \equiv_p -1$, если $m \vdots p-1$, либо $S \equiv_p 0$ в противном случае.(*Указание: домножьте всю сумму на n^m и посмотрите как она изменится.*)

2. Пусть $F(x_1,\dots,x_n)\in\mathbb{Z}[x_1,\dots,x_n]$ и $\deg F < n(p-1)$. Тогда

$$\sum_{k_1,\dots,k_n\in\mathbb{Z}_p} F(k_1,\dots,k_n) \equiv_p 0.$$

(*Указание: так как утверждение должно быть верно для любого многочлена с целыми коэффициентами, то оно должно быть верно и для монома.*)

Теорема 1 (Теорема Варнинга)**.** *Если степень r многочлена $F(x_1,\dots,x_n)\in\mathbb{Z}[x_1,\dots,x_n]$ меньше n, то число решений сравнения $F(x_1,\dots,x_n)\equiv_p 0$ кратно p.*

(Указание: рассмотрие многочлен $1-F^k$, чему надо взять равным параметр k нужно догадаться.)

Теорема 2 (Теорема Шевале)**.** *Пусть $F(x_1,\dots,x_n)\in\mathbb{Z}[x_1,\dots,x_n]$ многочлен с нулевым свободным членом и $\deg F(x_1,\dots,x_n)<n$, то сравнение*

$$F(x_1,\dots,x_n)\equiv_p 0.$$

имеет ненулевое решение.

Определение 1. Пусть $a\in\mathbb{Z}_n, (a,n)=1$, тогда показателем a называется наименьшее натуральное l такое, что $a^l\equiv_n 1$.

3. а) Рассмотрим уравнение $x^l-1\equiv_p 0$. Известно, что при $l=p-1$ это уравнение имеет ровно l корней в $\mathbb{Z}_p$. Докажите это утверждение для любого l, являющегося делителем $p-1$.

б) Докажите, что решения уравнения $x^l-1\equiv_p 0$, являются остатки, показатели которых делят l.

в) Докажите, что $n=\sum_{l|n}\varphi(l)$. (*Указание: например это можно сделать индукцией по кол-ву простых множетелей в разложении числа n.*)

г) Докажите, что число решений уранения $x^l-1\equiv_p 0$, где $l|p-1$ с показателем l равно $\varphi(l)$. (*Указание:индукция всех спасёт.*)

д) Докажите, что первообразных корней по простому модулю $\varphi(p)$ штук.