Многочлены над Z_p

Определение 1. Через $\mathbb{Z}_p$ мы будем обозначать множество остатков по модулю p, с операциями «$+$» и «$\cdot$», которые по двум остаткам a и b, выдают новый остаток r, сравнимый с $r \underset{p}{\equiv} a+b$ и $r \underset{p}{\equiv} ab$ соответственно.

1. Пусть p — простое число. а) Докажите, что $\mathbb{Z}_p$ поле. б) Докажите, что в кольце многочленов $\mathbb{Z}_p[x]$ выполнена теорема Безу. Докажите, что у не нулевого многочлена из $\mathbb{Z}_p[x]$ различных корней не больше, чем его степень. Сформулируйте результат этой задачи для колец многочленов $K[x]$, где K — поле.

2. а) Докажите равенство многочленов $x^p - x = x(x-1)(x-2)\cdot\ldots\cdot(x-(p-1))$. С помощью предыдущего пункта докажите следующие задачи.
б) Докажите теорему Вильсона: $(p-1)! \underset{p}{\equiv} -1$.

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

4. Докажите, что любую функцию над $Z_p \to Z_p$ можно задать многочленом степени не выше $p+1$.

5. Докажите, что для любого натурального а) $0 < m < p-1$; б) $m \not\vdots p-1$ существует такое n, что $(n,p) = 1$, $n^m \not\underset{p}{\equiv} 1$.
в) Пусть m — натуральное число. Рассмотрим сумму

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

Тогда либо $S \underset{p}{\equiv} -1$, если $m \vdots p-1$, либо $S \underset{p}{\equiv} 0$ в противном случае.