Остатки и коэффициенты многочленов

Деление остатков

Далее всюду p – простое число.

Опр. $\mathbf{Z}_p$ – множество остатков. В нем корректно определены сложение, вычитание и умножение, а также деление на остаток, не равный 0.

Упр1. Найдите 2/7 mod 11, 4/18 mod 19, 11/5 mod 101.

Упр2. Найдите все остатки по модулю p, обратные самим себе.

Зад3. а) Найдите сумму $1/1+1/2+\ldots+1/(p-1)$ в $\mathbf{Z}_p$.

б) Сумму дробей $1/1, 1/2, \ldots, 1/(p-1)$ привели к общему знаменателю. Докажите, что числитель делится на p, если p — нечетное.

в) Сумму дробей $1/1^2, 1/2^2, \ldots, 1/(p-1)^2$ привели к общему знаменателю. Докажите, что числитель делится на p, если $p>3$.

Зад4. Пусть a и b – два остатка из $\mathbf{Z}_p$.
а) Докажите, что $(a+b)^p=a^p+b^p$.
б) Выведите из (а) Малую теорему Ферма.

Зад5. Пусть p и q — простые, $q > 5$. Известно, что $2^p + 3^p$ делится на q. Докажите, что $q > 2p$.

Многочлены с коэффициентами из $\mathbf{Z}_p$

Опр. $\boldsymbol{K}[x]$ – множество многочленов с коэффициентами из множества $\boldsymbol{K}$.

Упр6. а) Докажите, что $\mathbf{Z}[x]$ и $\mathbf{Z}_p[x]$ замкнуты относительно сложения, вычитания и умножения.
б) Замкнуто ли $\mathbf{Z}[x]$ относительно деления с остатком, если старший коэффициент делителя равен 1?
в) Замкнуто ли $\mathbf{Z}_p[x]$ относительно деления с остатком?
г) Верна ли для многочленов из $\mathbf{Z}_p[x]$ теорема Безу?
д) Может ли у многочлена степени n из $\mathbf{Z}_p[x]$ быть более n корней?

Зад.7 а) Докажите, что в $\mathbf{Z}_p[x]$ верно равенство $x^{p-1}-1 = (x-1)(x-2)\ldots(x-(p-1))$.
б) Выведите из (а) теорему Вильсона.

Зад.8 а) Пусть $F(x)$ – многочлен из $\mathbf{Z}_p[x]$. Докажите, что $F(x)^p = F(x^p)$.

б) Выведите из (а), что $C^k_{p^n}$ кратно p при $k\neq 0, p^n$.

Зад.9 Найдите количество коэффициентов $(x+1)^{100}$, кратных 2.

На дом

ОП1. $f, g\in \mathbf{Z}_p[x]$. Известно, что для любого $k\in\mathbf{Z}_p$ $f(k)=g(k)$. Обязательно ли у f и g равны степени и все коэффициенты?

ОП2. Докажите, что для любого р в $\mathbf{Z}_p[x]$ есть многочлен без корней
а) степени 2;
б) любой степени от p и выше.

ОП3. Докажите, что
а) в Z_p для любого $n>1$ есть не более $n-1$ остатка с показателем n;
б) в Z_{47} есть не менее 23 остатков с показателем 46.