9 класс, многочлены $\mathbb{Z}_p[x]$ и первообразные корни по модулю, теория, 9 июля

Определение. Число *g* называется *первообразным корнем* по модулю *m*, если все $a \in Z_m^*$ являются различными степенями *g*. *(Более правильно: первообразным корнем является не число, а его остаток, вычет).*

Определение. Число *g* называется *первообразным корнем* по модулю *m*, если показатель *g* по mod *m* равен φ (*m*).

Поймите, почему определения эквивалентны.

Далее мы будем заниматься случаем простого модуля. Основная цель – понять, есть ли вообще первообразный корень.

Т1. Пусть *P*(*x*) – многочлен степени *n*, со старшим коэффициентом равным 1. Докажите, что при простом p сравнению *P*(*x*) ≡ 0 (mod *p*) удовлетворяет не более, чем *n* различных остатков (классов вычетов). *(Указание – воспользуйтесь теоремой Безу для остатков и индукцией по n).*

Вопрос на понимание как раскладывается на простые множители многочлен $x^{p-1}-1$ (как многочлен с коэффициентами в остатках по модулю p).

Т2. Докажите, что порядок *d* имеет не более *φ*(*d*) элементов Z_p^* . (например, вы можете перечислить их, а дальше допустить, что есть и другие).

Т3. Вспомните доказательство тождества Гаусса.

Т4. Пусть *p* – простое число , а *d* – делитель числа *p*–1. Тогда ровно *φ*(*d*) элементов Z_p^* имеет порядок *d*.

Т5. Пусть *x* имеет порядок *a*, а *y* имеет порядок *b*. Докажите, что если НОД(*a,b*) = 1, то *xy* имеет порядок *ab.*

Следствие *Для каждого простого p существует φ(p –1) первообразных корней.*

Упражнение 1. Найдите все первообразные корни а) по модулю 7; б) по модулю 13.

Тридцать третья Летняя Многопредметная Школа Кировской области
Вишкиль. 3-28 июля 2017 года.

9 класс, многочлены $\mathbb{Z}_p[x]$ и первообразные корни по модулю, теория, 9 июля

Определение. Число *g* называется *первообразным корнем* по модулю *m*, если все $a \in Z_m^*$ являются различными степенями *g*. *(Более правильно: первообразным корнем является не число, а его остаток, вычет).*

Определение. Число *g* называется *первообразным корнем* по модулю *m*, если показатель *g* по mod *m* равен φ (*m*).

Поймите, почему определения эквивалентны.

Далее мы будем заниматься случаем простого модуля. Основная цель – понять, есть ли вообще первообразный корень.

Т1. Пусть *P*(*x*) – многочлен степени *n*, со старшим коэффициентом равным 1. Докажите, что при простом p сравнению *P*(*x*) ≡ 0 (mod *p*) удовлетворяет не более, чем *n* различных остатков (классов вычетов). *(Указание – воспользуйтесь теоремой Безу для остатков и индукцией по n).*

Вопрос на понимание как раскладывается на простые множители многочлен $x^{p-1}-1$ (как многочлен с коэффициентами в остатках по модулю p).

Т2. Докажите, что порядок *d* имеет не более *φ*(*d*) элементов Z_p^* . (например, вы можете перечислить их, а дальше допустить, что есть и другие).

Т3. Вспомните доказательство тождества Гаусса.

Т4. Пусть *p* – простое число , а *d* – делитель числа *p*–1. Тогда ровно *φ*(*d*) элементов Z_p^* имеет порядок *d*.

Т5. Пусть *x* имеет порядок *a*, а *y* имеет порядок *b*. Докажите, что если НОД(*a,b*) = 1, то *xy* имеет порядок *ab.*

Следствие *Для каждого простого p существует φ(p –1) первообразных корней.*

Упражнение 1. Найдите все первообразные корни а) по модулю 7; б) по модулю 13.