НЕПРИВОДИМОСТЬ МНОГОЧЛЕНОВ НАД КОНЕЧНЫМ ПОЛЯМИ

Куянбаева Карина[1], Булакова Феруза[2]

[1,2]Студентка 3-курса математического факультета Самаркандского Государственного Университета имени Шарофа Рашидова

e-mail: karinamath@mail.ru

Аннотация: в статье рассматривается неприводимость многочленов над конечными полями. В данной работе анализируется критерий Батлера для многочленов. Сперва излагаются фундаментальные понятия, а затем представленная информация подкрепляется примерами.

Ключевые слова: конечные поля, неприводимость, многочлен, критерий Батлера.

Если поле P конечно то над ним существует неприводимый многочлен любой степени. Это значительно усложняет решение вопроса о неприводимости многочлена над конечным полем. Критерий Батлера который был установленный М. Батлером в 1954-году дает легкое решение данного вопроса[1].

Конечное поле состоящие из q элементов существует тогда и только тогда, если q −простое число или степень какого-либо простого числа [2]. Здесь q − число элементов поля. Любое конечное поле называется *Полем Галуа* и обозначается как $GF(q)$. Далее мы рассмотрим формулировку Критерия Батлера и практический удобный способ распознавания приводимости и неприводимости многочленов над полем $GF(q)$.

Теорема(Критерий Батлера)[1]

Многочлен $f(x) \in P[x]$ степени n неприводим над полем $P = GF(q)$ тогда и только тогда, когда выполнены условия:

1)Унитарный НОД$(f, f') = 1$;

2)Уравнение $z^q - z = 0$ имеет в кольце $P[x]/f(x)$ ровно q решений.

Рассмотрим как пользоваться вышеуказанным критерием в практике:

1)Если НОД$(f, f') \neq 1$, то многочлен приводим на основание теоремы.

2)Если НОД$(f, f') = 1$. Тогда проверяем 2-условие теоремы. Для этого построим многочлены $\delta_i(x) \equiv x^{iq} - x^i \ (mod f), i = \overline{1, n-1}$, которые

$\delta_i(x) = \delta_{0i} + \delta_{1i}x + \cdots + \delta_{n-1,i}x^{n-1}$, то есть многочлен $\delta_i(x)$ остаток деления $x^{iq} - x^i$ на $f(x)$.

Из коэффициентов многочленов $\delta_i(x)$ составим матрицу A, столбцы которой состоят из коэффициентов соответствующих многочленов, при этом первый столбец всегда нулевой.

$$A = \begin{pmatrix} 0 & \delta_{01} & \cdots & \delta_{0,n-1} \\ 0 & \delta_{11} & \cdots & \delta_{1,n-1} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \delta_{n-1,1} & \cdots & \delta_{n-1,n-1} \end{pmatrix}$$

В силу Критерия Батлера многочлен $f(x)$ неприводим над $GF(q)$ тогда и только тогда, когда $rankA = n - 1$. В противном случае $f(x)$ –приводим.

ВАЖНО ЗНАТЬ!, что все операции связанные с делением многочленов, нахождение НОДа и вычисления ранга матрицы проводятся в конечном поле $GF(q)$, то есть по модулю q.[3]

Рассмотрим несколько примеров на практике с применением данного алгоритма.

Пример1.

Определить приводимы или нет многочлены $x^2 + 1$ и $x^3 + x + 1$ над полем $GF(2)$[4].

Решение. 1)Приведем решение для $f(x) = x^2 + 1$.

1)Сначала найдем НОД(f, f'). Значит $f' = 2x$. Используя алгоритм Эвклида имеем НОД$(f, f') = 1$. Так как 1-условие теоремы выполнено, то переходим к условию 2.

2)Построим многочлен $\delta_i(x) \equiv x^{iq} - x^i \ (modf), i = 1,$ так как степень многочлена равна $n = 2,$ а число элементов поля $q = 2$. Значит, степень многочлена $\delta_1(x) \equiv x^2 - x \ (modf)$, $\deg(\delta_1(x)) \leq 1$. Нам надо найти остаток деления $x^2 - x$ на $x^2 + 1$.Учитывая что поле $GF(2)$ содержит два элемента $\{0,1\}$, мы имеем $-1 \equiv 1(mod2)$, то есть $\delta_1(x) \equiv x^2 + x \ (modf)$. Выполняя деление уголком, находим остаток $x - 1$, то есть в поле $GF(2)$ $x + 1$. Отсюда вытекает, что $\delta_1(x) = x + 1$.

3)Составим матрицу A:

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}.$$

Вычислим ранг матрицы в поле $GF(2)$ и сравним его с числом 1:

$rankA = 1 = 1$. Следуя критерию Батлера многочлен $f(x)$ неприводим над полем $GF(2)$.

2)Решим для $g(x) = x^3 + x + 1$.

1)$g' = 3x^2 + 1$. В поле $GF(2)$ $g' = x^2 + 1$. Пользуясь алгоритмом Эвклида находим НОД$(g, g') = 1$. Переходим к 2-условию.

2)Степень многочлена $g(x)$ равна 3, а число элементов поля 2. Построим многочлены $\delta_i(x) \equiv x^{i2} - x^i \ (modf), i = 1,2, \deg(\ \delta_i(x)) \leq 2$.

3)При $i = 1$ получаем $\delta_1(x) \equiv x^2 - x \ (modg)$. Переводя все коэффициенты в поле $GF(2)$, находим $\delta_1(x) = x^2 + x = 1 \cdot x^2 + 1 \cdot x + 0$.

4)При $i = 2$ получаем $\delta_2(x) \equiv x^4 - x^2\ (mod g)$. Пользуясь делением столбиком, находим $\delta_2(x) = -x$, а в поле $GF(2)$

$\delta_2(x) = x = 0 \cdot x^2 + 1 \cdot x + 0.$

5)Составим матрицу B:

$$B = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Ранг матрицы равен 2, то есть многочлен $g(x)$ приводим над полем $GF(2)$.

Пример 2.

Имеет ли уравнение $x^3 + x^2 + 1 = 0$ корни в поле $GF(3)$, если да то найти их.

Решение.1) Чтобы понять имеет ли данное уравнение корни в данном поле, представим что левая часть уравнения это многочлен, то есть

$p(x) = x^3 + x^2 + 1$ и проверим удовлетворяет ли он критерий Батлера. $p' = 3x^2 + 2x$, находим НОД$(p, p') = 1$. Переходим к условию 2.

2)$\deg\big(p(x)\big) = 3$ и число элементов поля $q = 3$, значит надо составить многочлены вида $\delta_i(x) \equiv x^{3i} - x^i\ (mod p), i = 1,2, \deg\big(\delta_i(x)\big) \leq 2.$

3)При $i = 1$ $\delta_1(x) \equiv x^3 - x\ (mod p)$, а в поле $GF(2)$ $\delta_1(x) \equiv x^3 + 2x\ (mod p)$. Пользуясь делением в столбик имеем $\delta_1(x) = 2x^2 + 2x + 2.$

4)При $i = 2$ $\delta_2(x) \equiv x^6 - x^2\ (mod p)$ а в поле $GF(3)$

$\delta_2(x) \equiv x^6 + 2x^2\ (mod p)$, так как $-1 \equiv 2(mod 3)$. Отсюда имеем остаток вида: $\delta_2(x) = 2x^2 + 2x + 2.$

5)Составим матрицу C:

$$C = \begin{pmatrix} 0 & 2 & 2 \\ 0 & 2 & 2 \\ 0 & 2 & 2 \end{pmatrix}.$$

Ранг матрицы равен 1, то есть $rankC < 2$. А значит многочлен приводим над полем.

6)После того как мы определили, что многочлен $p(x) = x^3 + x^2 + 1$ приводим над полем $GF(3)$, можно сказать что он имеет корни в данном поле. А это значит что у уравнения есть решения в поле $GF(3)$. Подставляя элементы

$\{0,1,2\}$ в уравнение можно убедиться, что $x = 1$ корень уравнения.

Следствие1. С помощью приводимости и корней многочлена можно разложить многочлен на неприводимые множители в конечных полях. Например для многочлена $p(x) = x^3 + x^2 + 1$ корень $x = 1$ и разделив многочлен на $x - 1 = x + 2$ мы имеем $p(x) = (x + 2)(x^2 + 2x + 2)$, множитель $x^2 + 2x + 2$ не имеет корней в $GF(3)$, значит он неприводим над полем. Таким образом мы разложили многочлен на неприводимые множители в конечным поле.

СПИСОК ЛИТЕРАТУРЫ

1.Майорова.С., Завгородний.М. Методическое указание для организации самостоятельной работы по дисциплине «Алгебра и геометрия», Воронеж 2015.

2. Maurice R. Kibler. Galois field and Galois Rings made easy, Copyright © 2017 ISTE Press Ltd. Published by Elsevier Ltd.

3.Ишмухаметов.Ш, Рубцова.Р. Вычисления конечных полях. Казань 2019.

4.Осипов.Н., Медведева. М., Многочлены над конечными полями, Красноярск СФУ 2016.

5.Кострикин.А. Введение в алгебру