

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ



Студенттер мен жас ғалымдардың
«ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2016» атты
XI Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XI Международной научной конференции
студентов и молодых ученых
«НАУКА И ОБРАЗОВАНИЕ - 2016»

PROCEEDINGS
of the XI International Scientific Conference
for students and young scholars
«SCIENCE AND EDUCATION - 2016»

2016 жыл 14 сәуір
Астана

**ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ**

**Студенттер мен жас ғалымдардың
«Ғылым және білім - 2016»
атты XI Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ**

**СБОРНИК МАТЕРИАЛОВ
XI Международной научной конференции
студентов и молодых ученых
«Наука и образование - 2016»**

**PROCEEDINGS
of the XI International Scientific Conference
for students and young scholars
«Science and education - 2016»**

2016 жыл 14 сәуір

Астана

ӘӨЖ 001:37(063)

КБЖ 72:74

Ғ 96

Ғ96 «Ғылым және білім – 2016» атты студенттер мен жас ғалымдардың ХІ Халық. ғыл. конф. = ХІ Межд. науч. конф. студентов и молодых ученых «Наука и образование - 2016» = The XI International Scientific Conference for students and young scholars «Science and education - 2016» . – Астана: [http://www.enu.kz/ru/nauka/ nauka-i-obrazovanie/](http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/), 2016. – б. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-764-4

Жинаққа студенттердің, магистранттардың, докторанттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

ӘӨЖ 001:37(063)

КБЖ 72:74

ISBN 978-9965-31-764-4

©Л.Н. Гумилев атындағы Еуразия
ұлттық университеті, 2016

МНОГОЧЛЕНЫ НАД КОНЕЧНЫМИ ПОЛЯМИ

Коротоква Асель Сериковна

assel92.kz@mail.ruМагистрант механико-математического факультета ЕНУ им.Л.Н.Гумилева, Астана,
Казахстан

Научный руководитель – Ахметжанова К.О.

В работе используются определения и обозначения из книги [1].

Любой непостоянный многочлен над заданным полем F можно разложить в произведение неприводимых многочленов. Если рассматриваемое поле F конечно, то для вычисления неприводимых сомножителей многочлена положительной степени над этим полем существуют эффективные алгоритмы. Существование таких алгоритмов разложения многочленов над конечными полями особенно важно для приложений теории конечных полей: для теории кодирования, для изучения линейных рекуррентных соотношений в конечных полях и др. Кроме того, в алгебре и теории чисел есть много вычислительных задач, которые связаны с разложением многочленов над конечными полями, например, вычисление группы Галуа некоторого уравнения над полем рациональных чисел и др.

Один из таких алгоритмов известен как алгоритм Берлекэмп [2].

Проблему разложения многочлена положительной степени над заданным полем можно свести к задаче разложения некоторого числа многочленов, не имеющих кратных неприводимых сомножителей. Это позволяет нам сосредоточить свое внимание на многочленах, не имеющих кратных неприводимых сомножителей. Следующая теорема является основной.

Теорема 1 [1]. Если $f \in \mathbb{F}_q[x]$ – нормированный многочлен положительной степени и многочлен $h \in \mathbb{F}_q[x]$ удовлетворяет условию $h^q \equiv h \pmod{f}$, то

$$f(x) = \prod_{c \in \mathbb{F}_q} \text{НОД}(f(x), h(x) - c). \quad (1)$$

Поскольку разложение, основанное на формуле (1), связано с вычислением q наибольших общих делителей, то прямое применение этой формулы возможно лишь для малых конечных полей $\mathbb{F}_q$ (т.е. для небольших значений q). Алгоритм Берлекэмп непригоден для случая, когда число элементов поля велико. Поэтому необходимо найти пути сокращения числа элементов $c \in \mathbb{F}_q$, для которых в формуле (1) нужно подсчитывать наибольшие общие делители. Отметим, что мы считаем порядок q конечного поля $\mathbb{F}_q$ «большим», если он существенно больше степени разлагаемого многочлена.

Рассмотрим алгоритм разложения многочлена над большими полями, который носит название алгоритм Цассенхауза.

Пусть f – произвольный нормированный многочлен степени n из кольца $\mathbb{F}_q[x]$, разлагающийся в произведение k различных нормированных неприводимых сомножителей над полем $\mathbb{F}_q$. Допустим, что многочлен $h \in \mathbb{F}_q[x]$ удовлетворяет условиям $h^q \equiv h \pmod{f}$ и $0 < \deg(h) < n$, так что он является f -разлагающим многочленом. Так как различные наибольшие общие делители из правой части формулы (1) взаимно просты, то не более k из них могут быть отличны от 1. Задача состоит в том, как охарактеризовать те элементы $c \in \mathbb{F}_q$, для которых $\text{НОД}(f(x), h(x) - c) \neq 1$.

Существуют различные методы таких характеристик.

Одну из таких характеристик можно получить, применяя теорию результатов.

Определение 1. Пусть $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n \in K[x]$ и $g(x) = b_0x^m + b_1x^{m-1} + \dots + b_m \in K[x]$ – два многочлена с формальными степенями n и m соответственно, $n, m \in \mathbb{N}$. Тогда результат $R(f, g)$ этих двух многочленов – это определитель

$$R(f, g) = \begin{vmatrix} a_0 & a_1 & \dots & a_n & 0 & \dots & \dots & 0 \\ 0 & a_0 & \dots & \dots & a_n & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & a_0 & a_1 & \dots & \dots & a_n \\ b_0 & b_1 & \dots & \dots & b_m & 0 & \dots & 0 \\ 0 & b_0 & \dots & \dots & \dots & b_m & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & \dots & b_0 & b_1 & \dots & \dots & b_m \end{vmatrix}$$

порядка $m + n$.

Пусть $R(f(x), h(x) - c)$ - результат многочленов $f(x)$ и $h(x) - c$, где в качестве формальных степеней берутся степени этих многочленов. Тогда $\text{НОД}(f(x), h(x) - c) \neq 1$ в том и только в том случае, если $R(f(x), h(x) - c) = 0$. Так мы приходим к рассмотрению функции

$$F(y) = R(f(x), h(x) - y),$$

которая является многочленом степени, не большей n , относительно переменной y . Ясно, что $\text{НОД}(f(x), h(x) - c) \neq 1$ в том и только том случае, если элемент c является корнем многочлена $F(y)$ из поля $\mathbb{F}_q$.

Многочлен $F(y)$ можно найти непосредственно из его определения: для этого потребуется вычислить определитель порядка не более чем $2n + 1$, элементами которого являются либо элементы из поля $\mathbb{F}_q$, либо линейные многочлены от y с коэффициентами из $\mathbb{F}_q$. Однако во многих случаях предпочтительнее другой способ, состоящий в следующем. Выберем $n + 1$ различных элементов $c_0, c_1, \dots, c_n$ из $\mathbb{F}_q$ и подсчитаем результаты $r_i = R(f(x), h(x) - c_i)$, $i = 0, 1, \dots, n$. Тогда тот единственный многочлен $F(y)$ степени, не превосходящей n , для которого $F(c_i) = r_i$, $i = 0, 1, \dots, n$, можно получить с помощью интерполяционной формулы Лагранжа.

Теорема 2. (интерполяционная формула Лагранжа). Пусть $n \geq 0$ и пусть $a_0, a_1, \dots, a_n$ - различные и $b_0, b_1, \dots, b_n$ - произвольные элементы поля F . Тогда существует в точности один многочлен $f \in F$ степени $\leq n$, такой, что $f(a_i) = b_i$ для $i = 0, 1, \dots, n$. Этот многочлен имеет вид

$$f(x) = \sum_{i=0}^n b_i \prod_{\substack{k=0 \\ k \neq i}}^n (a_i - a_k)^{-1} (x - a_k).$$

Этот метод имеет еще то преимущество, что если какие-либо элементы r_i равны нулю, то мы автоматически получаем корни многочлена $F(y)$ из поля $\mathbb{F}_q$. Тогда вопрос о выделении тех элементов $c \in \mathbb{F}_q$, для которых $\text{НОД}(f(x), h(x) - c) \neq 1$, сводится к вопросу нахождения корней некоторого многочлена в поле $\mathbb{F}_q$.

Другой метод характеристики тех элементов c поля $\mathbb{F}_q$, для которых нужно подсчитывать $\text{НОД}(f(x), h(x) - c)$ в формуле (1), основан на следующих соображениях. Пусть S обозначает множество всех тех $c \in \mathbb{F}_q$, для которых $\text{НОД}(f(x), h(x) - c) \neq 1$. Тогда из (1) следует, что

$$f(x) = \prod_{c \in S} \text{НОД}(f(x), h(x) - c), \quad (2)$$

так что многочлен $f(x)$ делит произведение $\prod_{c \in S} (h(x) - c)$. Введем в рассмотрение многочлен

$$G(y) = \prod_{c \in S} (y - c)$$

Тогда многочлен $f(x)$ делит $G(h(x))$ и многочлен $G(y)$ можно охарактеризовать следующим образом.

Теорема 3 [1]. Среди всех многочленов $g \in \mathbb{F}_q[y]$, таких, что $f(x)$ делит $g(h(x))$, многочлен $G(y)$ однозначно определяется тем, что это нормированный многочлен наименьшей степени.

Этот результат можно использовать следующим образом. Пусть m – число элементов множества C . Тогда запишем

$$G(y) = \prod_{c \in C} (y - c) = \sum_{j=0}^m b_j y^j$$

с коэффициентами $b_j \in \mathbb{F}_q$. Поскольку $f(x)$ делит $G(h(x))$, то мы получаем

$$\sum_{j=0}^m b_j h(x)^j \equiv 0 \pmod{f(x)}$$

Так как $b_m = 1$, то это сравнение можно рассматривать как нетривиальное соотношение линейной зависимости над полем $\mathbb{F}_q$, связывающее вычеты по модулю $f(x)$ многочленов $1, h(x), h(x)^2, \dots, h(x)^m$. Согласно теореме 3, если произвести нормирование так, чтобы $b_m = 1$, то такое соотношение линейной зависимости определяется однозначно; поэтому вычеты по модулю $f(x)$ многочленов $1, h(x), h(x)^2, \dots, h(x)^{m-1}$ линейно независимы над $\mathbb{F}_q$. Ограничение $m \leq k$ вытекает из (2).

Поэтому многочлен G можно найти, если приводить по модулю $f(x)$ степени многочлена $h(x)$: $1, h(x), h(x)^2, \dots$, пока не найдем ту наименьшую степень $h(x)^m$ этого многочлена, которая линейно зависит (над полем $\mathbb{F}_q$) от предыдущих степеней. Коэффициенты этого первого соотношения линейной зависимости в нормированной форме (т.е. с коэффициентом 1 при $h(x)^m$) и являются коэффициентами многочлена G . При этом для нахождения этого соотношения линейной зависимости требуется рассмотреть лишь степени многочлена $h(x)$ не выше k -й, где число k можно получить из алгоритма Берлекэмп. Элементами множества C являются корни многочлена G , лежащие в поле $\mathbb{F}_q$, и только они.

Этот метод, сводящий проблему нахождения элементов множества C к задаче отыскания корней некоторого многочлена в поле $\mathbb{F}_q$, носит название алгоритм Цассенхауза.

Построим пример реализации алгоритма Цассенхауза.

Пример 1. Найти каноническое разложение многочлена

$$f(x) = x^6 - 3x^5 + 5x^4 - 9x^3 - 5x^2 + 6x + 7 \in \mathbb{F}_{23}[x].$$

Так как $\text{НОД}(f(x), f'(x)) = 1$, то многочлен $f(x)$ не имеет кратных сомножителей. Применяя алгоритм Берлекэмп, найдем степени x^{23i} по модулю $f(x)$ для $i = 0, 1, \dots, 5$. Это приводит к матрице 6×6 .

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 5 & 0 & -1 & 8 & -3 & -10 \\ -10 & 10 & 10 & 0 & 1 & -9 \\ 0 & 7 & 9 & -8 & 10 & -11 \\ 11 & 0 & -4 & 7 & 7 & 2 \\ -3 & 0 & -10 & 9 & 2 & -9 \end{pmatrix},$$

так что матрица $B-I$ имеет вид

$$B-I = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 5 & -1 & -1 & 8 & -3 & -10 \\ -10 & 10 & 9 & 0 & 1 & -9 \\ 0 & 7 & 9 & -9 & 10 & -11 \\ 11 & 0 & -4 & 7 & 6 & 2 \\ -3 & 0 & -10 & 9 & 2 & -10 \end{pmatrix}.$$

Приведением этой матрицы элементарными преобразованиями столбцов к ступенчатому виду получаем, что ранг r матрицы $B-I$ равен 3, так что многочлен f имеет $k = 6 - r = 3$ различных нормированных неприводимых сомножителя над полем $\mathbb{F}_{23}$. Базис пространства решений однородной системы уравнений, соответствующий матрице $B-I$, задается векторами $h_1 = (1, 0, 0, 0, 0, 0)$, $h_2 = (0, 4, 2, 1, 0, 0)$ и $h_3 = (0, -2, 9, 0, 1, 1)$, которые

соответствуют многочленам $h_1(x) = 1$, $h_2(x) = x^3 + 2x^2 + 4x$, $h_3(x) = x^5 + x^4 + 9x^2 - 2x$. Возьмем в качестве f -разлагающего многочлена $h_2(x) = x^3 + 2x^2 + 4x \in \mathbb{F}_{23}[x]$. Применим теперь алгоритм Цассенхауза для нахождения множества C тех элементов $c \in \mathbb{F}_{23}$, для которых $\text{НОД}(f(x), h(x) - c) \neq 1$. Мы имеем

$$h_2(x) \equiv x^3 + 2x^2 + 4x \pmod{f(x)},$$

$$h_2(x)^2 \equiv 7x^5 + 7x^4 + 2x^3 - 2x^2 - 6x - 7 \pmod{f(x)}$$

так что $h_2(x)^2$ не зависит линейно от 1 и $h_2(x)$. Поскольку число m элементов множества C не превосходит $k = 3$, то степень $h_2(x)^3$ должна быть наименьшей степенью многочлена $h_2(x)$, которая линейно зависит от предыдущих степеней. Получаем

$$h_2(x)^3 \equiv -11x^5 - 11x^4 - x^3 - 9x^2 - 5x - 2 \pmod{f(x)}$$

и искомая линейная зависимость такова:

$$h_2(x)^3 - 5h_2(x)^2 + 11h_2(x) - 10 \equiv 0 \pmod{f(x)}$$

следовательно, $G(y) = y^3 - 5y^2 + 11y - 10$. Методом перебора вычетов по модулю 23 находим корни многочлена G в поле $\mathbb{F}_{23}[x]$: ими являются элементы 2, -3 и 6. Вычислим

$$\text{НОД}(f(x), h_2(x) - 2) = x^2 - x + 7,$$

$$\text{НОД}(f(x), h_2(x) + 3) = x - 4,$$

$$\text{НОД}(f(x), h_2(x) - 6) = x^3 + 2x^2 + 4x - 6$$

так что каноническим разложением многочлена $f(x)$ в кольце $\mathbb{F}_{23}[x]$ является

$$f(x) = (x - 4)(x^2 - x + 7)(x^3 + 2x^2 + 4x - 6).$$

По материалам исследований темы «Многочлены над конечными полями» автором разработан факультатив для учащихся старших классов школ с углубленным изучением математики. Материал факультатива может также использоваться в вузах в качестве элективных дисциплин по алгебре и дискретной математике.

Список использованных источников

1. Лидл Р., Нидеррайдер Г. Конечные поля. Том 1. – М.: Мир, 1988.
2. Берлекэмп Э. Алгебраическая теория кодирования. – М.: Мир, 1971.

ӘОК 377

МАТЕМАТИКАНЫ ОҚЫТУДА ТЕХНОЛОГИЯЛЫҚ КАРТАЛАРДЫ ҚҰРАСТЫРУДЫҢ БІР ӘДІСІ

¹Қайрат Бекболат, ²Муталип Риза

¹Л.Н.Гумилев атындағы ЕҰУ, 2 курс магистранты, Астана, Қазақстан.

²Л.Н.Гумилев атындағы ЕҰУ, алгебра және геометрия кафедрасының оқытушысы,
Астана, Қазақстан

Ғылыми жетекші – А.С. Сарсекеев

Ұсынылып отырған карта арқылы кез келген пән мұғалімі сабақты бастау барысында оқушыларға тақырыпты толық ашу үшін осы картаны пайдаланса онда оның сабағы әрі түсінікті әрі тақырыбы толық ашыла түседі деген ойдамыз. Енді осы жоғарыдағы беріліп отырған картаның қандай мақсатта пайдалану керек екеніне тоқтала кетейік. Технологиялық карта бірнеше фигуралардан құралған және схема арқылы көрсетілген. Ортасындағы шеңберге жету үшін фигуралар өзгеріп отырады алдымен үшбұрыш содан кейін төртбұрыш сосын бесбұрыш, алтыбұрыш, сегізбұрыш т.с.с. Яғни бұрыштарының саны неғұрлым көбейген сайын берілген тақырыпты кеңейте түседі және толық ашыла түседі. Осы карта арқылы пән мұғалімі оқушыларға тақырыпты толық ашып көрсете алады. Енді картаны қалай пайдалану керектігіне тоқталайық. Ол үшін біз осы карта арқылы бір тақырыпты алып