Конечные поля, открытые Эваристом Галуа (поэтому нередко их именуют полями Галуа) в первой трети XIX-го столетия, на протяжении большей части своей истории считались пригодными в основном для иллюстрации свойств «настоящих» (бесконечных) полей. И лишь в последние десятилетия резко возросло прикладное значение конечных полей, в первую очередь благодаря бурному развитию теории кодирования. Еще одной важной причиной, приведшей к переоценке роли теории конечных полей, явилось открытие Берлекэмпом в 1967 году очень быстрого алгоритма факторизации многочленов над конечными полями. Этот алгоритм является важной составной частью одного из лучших методов факторизации полиномов с рациональными коэффициентами.

Вычисления в конечных полях играют переходную роль от перечислительных, комбинаторных методов математики конечных объектов к классической компьютерной алгебре. Вычисления ведутся в конечном множестве, но переборный подход в основном уступает место иному, когда мы по мере решения задачи вычисляем и храним в памяти лишь отдельные элементы изучаемого множества. В этом смысле расчеты в конечных полях идентичны вычислениям в бесконечной области. Однако в случае конечных полей не составляет труда представить вычисляемые элементы в каноническом виде, поэтому в этой ситуации не возникает проблем, связанных с идентификацией и «разбуханием» данных, характерных для бесконечного случая.

Некоторые сведения из алгебры

В этом параграфе приведены сведения из курсов алгебры и теории чисел, необходимые для понимания основного материала.

Непустое множество, на котором задана ассоциативная бинарная операция называется **полугруппой**.

Полугруппа, обладающая нейтральным элементом, называется **моноидом.**

Моноид, в котором каждый элемент имеет обратный, называется **группой.**

Группа, в которой операция коммутативна, называется **абелевой.**

Группа называется **циклической**, если она порождена одним элементом. Иными словами, каждый элемент циклической группы есть степень некоторого фиксированного элемента, называемого порождающим, с целым показателем.

Циклическая группа обязательно является абелевой.

Непустое множество A, на котором заданы две бинарные операции + (сложение) и · (умножение), называется **кольцом** при условии что:

1. A – абелева группа по сложению;
2. A – полугруппа по умножению;
3. умножение дистрибутивно относительно сложения.

Кольцо называется **коммутативным**, если операция умножения обладает свойством коммутативности.

Элементы a и b кольца A называются **делителями нуля**, если сами они отличны от нуля, а их произведение равно нулю.

Ненулевое коммутативное кольцо с единицей называется **областью целостности**, если оно не содержит делителей нуля.

Аддитивная подгруппа I области целостности A называется **идеалом**, если произведение любого элемента из I на любой элемент из A всякий раз лежит в I. Множество кратных некоторому фиксированному элементу a из A является идеалом и называется главным идеалом, порожденным элементом a.

Элементы a и b области целостности A называются **сравнимыми по идеалу** I, если их разность принадлежит I. Элементы a и b, сравнимые по главному идеалу, порожденному элементом m, называют также сравнимыми по модулю m, и записывают этот факт так: $a \equiv b \pmod{m}$.

Отношение сравнимости по идеалу есть отношение эквивалентности. На фактормножестве (множестве классов эквивалентности) A/I естественным образом вводится операция сложения: суммой двух классов называется класс, содержащий сумму некоторых представителей слагаемых. Аналогичным образом вводится произведение классов. Легко показать, что определенные таким образом операции не зависят от выбора представителей в классах операндов и что относительно этих операций множество A/I (читается “A по I”) является кольцом. Это кольцо называется **факторкольцом** области целостности A по идеалу I. Это кольцо является коммутативным, обладает единицей, но в нем могут содержаться делители нуля. Поэтому факторкольцо A/I не обязано быть областью целостности.

Важный класс колец образуют области целостности, в которых справедлива теорема о делении с остатком. Такие кольца называют **евклидовыми**. В евклидовых кольцах имеет место следующее утверждение, называемое **китайской теоремой об остатках**:

Пусть элементы $a_1, a_2, ...,.a_n$ – попарно взаимно просты. Тогда для любого набора элементов $b_1, b_2, ...,.b_n$ найдется элемент c такой, что $c \equiv b_i \pmod{a_i}$, где i пробегает множество {1, 2, ..., n}. Причем эле-

мент c, обладающий указанными свойствами, определен однозначно по модулю $a_1 \cdot a_2 \cdot \ldots \cdot a_n$.

Область целостности, содержащая более одного элемента, называется **полем**, если каждый ее ненулевой элемент обратим.

Множество ненулевых элементов поля образует группу по умножению. Эту группу называют мультипликативной группой поля.

Пусть F – поле. Наименьшее натуральное число p такое, что сумма p единиц из F равняется нулю, называется **характеристикой поля** F. Если же такого числа не существует, говорят, что поле F имеет нулевую характеристику.

Два поля F и E называются **изоморфными**, если существует биективное отображение $\varphi: F \to E$ такое, что для любых элементов a и b поля F выполняются соотношения: $\varphi(a + b) = \varphi(a) + \varphi(b)$ и $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$. Само отображение φ называют при этом изоморфизмом поля F на поле E. Изоморфизм поля на себя называется **автоморфизмом** этого поля.

Если поле F содержится в поле E, то F называют **подполем** поля E, а E, в свою очередь, называют **расширением** поля F. Поле F называется **простым**, если оно не содержит собственных подполей (т. е. подполей, отличных от F).

Множество многочленов от одной переменной x с коэффициентами из поля F является евклидовым кольцом и обозначается F[x].

Многочлен f(x) из F[x] делится на двучлен x-a тогда и только тогда, когда элемент a является корнем f(x). Это утверждение называется **следствием из теоремы Безу**.

Непостоянный многочлен называется **неприводимым** над полем F, если его нельзя представить в виде произведения двух непостоянных многочленов из F[x].

Всякий непостоянный многочлен из F[x] единственным образом (с точностью до порядка сомножителей и ненулевых множителей из F) представляется в виде произведения степеней различных неприводимых многочленов.

Абелева группа V (по сложению) называется **векторным (линейным) пространством** над полем F, если на V задана внешняя операция умножения на скаляры из F, обладающая следующими свойствами:

1. $\forall a \in V \ \ \forall \alpha, \beta \in F \ \ \alpha(\beta a) = (\alpha\beta)a$;
2. $\forall a, b \in V \ \ \forall \alpha \in F \ \ \alpha(a + b) = \alpha a + \alpha b$;
3. $\forall a \in V \ \ \forall \alpha, \beta \in F \ \ (\alpha+\beta)a = \alpha a + \beta a$;
4. $\forall a \in V \ \ 1a = a$.

Векторы $a_1, a_2, \ldots, a_n$ называются **линейно независимыми**, если линейная комбинация этих векторов обращается в нуль только в

случае, когда все коэффициенты этой линейной комбинации равны нулю, и линейно зависимыми в противном случае. Очевидно, что векторы a_1, a_2, ..., a_n (n>1) являются линейно независимыми, если ни один из них не представляется в виде линейной комбинации остальных, и линейно зависимыми, если хотя бы один из них является линейной комбинацией остальных.

Векторное пространство называется **конечномерным**, если в нем существует конечная система порождающих, т. е. если каждый вектор пространства представляется в виде линейной комбинации фиксированной конечной системы векторов.

Упорядоченная линейно независимая система порождающих a_1, a_2, ..., a_n конечномерного линейного пространства V называется **базисом** это пространства. Во всех базисах V поровну векторов. Количество векторов базиса называется размерностью пространства. Одновременно размерность пространства есть максимально возможное число векторов в линейно независимой системе векторов и минимально возможное число векторов в системе порождающих пространства V.

Каждый вектор n-мерного пространства V единственным образом представляется в виде линейной комбинации базисных векторов. Коэффициенты этой линейной комбинации называются **координатами** данного вектора в данном базисе. Задание базиса устанавливает биективное соответствие между элементами V и всеми упорядоченными n-ками элементов из F. При сложении векторов складываются их одноименные координаты, а при умножении вектора на скаляр все его координаты умножаются на этот скаляр. Декартова n-ая степень F^n с заданными подобным образом операциями является n-мерным векторным пространством над F.Всякое n-мерное векторное пространство над F изоморфно этому пространству.

Множество решений однородной системы линейных уравнений от n неизвестных с коэффициентами из F образует подпространство пространства F^n. Размерность этого подпространства равна n-r , где r – ранг матрицы системы.

На любое расширение E поля F можно смотреть как на линейное пространство над F. Если это пространство конечномерно, то расширение E называют конечным, а размерность E над F называют степенью расширения.

Всякое конечное расширение E произвольного поля F является **алгебраическим**. Иными словами, каждый элемент из E является корнем некоторого полинома с коэффициентами из F. Множество полиномов, для которых данный элемент является корнем, образует главный идеал кольца многочленов от одной переменной над F, а

порождающий элемент этого идеала называется **минимальным неприводимым многочленом** данного элемента из E над F.

Если E конечное расширение поля K, а K конечное расширение поля F, то и E конечно над F, причем степень расширения E над F равна произведению степеней E над K и K над F. Это, так называемая, **теорема о башне расширений.**

Факторкольцо кольца многочленов F[x] по главному идеалу, порожденному неприводимым над F многочленом f(x), является полем. В это поле изоморфно вкладывается поле F, поэтому его обычно считают расширением F. В этом расширении многочлен f(x) имеет по крайней мере один корень α (это просто класс вычетов, порожденный многочленом x). Полученное таким образом расширение называется **простым алгебраическим расширением** поля F с помощью элемента α и обозначается $F(\alpha)$. Если степень полинома f(x) равна n, то такова же и степень расширения $F(\alpha)$, а элементы $1,\alpha, \alpha^2,\ldots,\alpha^{m-1}$ образуют базис $F(\alpha)$ над F. Этот базис называется **полиномиальным.**

Для всякого непостоянного многочлена f(x) из F[x] существует такое конечное расширение поля F, над которым f(x) раскладывается на линейные множители. Наименьшее (по включению) из таких полей называется **полем разложения** многочлена f(x). Поле разложения определено однозначно с точностью до изоморфизма, тождественного на F.

Корень α многочлена f(x) имеет **кратность** k, если f(x) делится на $(x - \alpha)^k$ и не делится на $(x - \alpha)^{k+1}$. Заметим, что α может не принадлежать основному полю, а лежать в поле разложения. Если $k>1$, то корень называется кратным. Кратные корни многочлена являются корнями его производной. Поэтому многочлен f(x) имеет кратные корни тогда и только тогда, когда он имеет нетривиальный наибольший общий делитель со своей производной.

Алгебраическое расширение E поля F называется **нормальным,** если каждый неприводимый над F многочлен, имеющий в E хотя бы один корень, разлагается над E на линейные множители. Поле разложения любого многочлена из F[x] является нормальным расширением поля F.

Алгебраическое расширение E поля F называется **сепарабельным,** если все его элементы являются простыми (не кратными) корнями своих неприводимых полиномов над F.

Множество автоморфизмов нормального сепарабельного расширения E поля F, действующих тождественно на элементы поля F является группой относительно операции композиции. Эта группа называется **группой Галуа.**

Результантом многочленов $a(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ и $b(x) = b_m x^m + b_{n-1}x^{n-1} + ... + b_1 x + b_0$ называется определитель порядка n+m, составленный из коэффициентов этих многочленов следующим образом:

$$R(a,b) = \begin{vmatrix} a_n & a_{n-1} & \dots & a_0 & 0 & \dots & \dots & 0 \\ 0 & a_n & \dots & a_1 & a_0 & 0 & \dots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \dots & 0 & a_n & a_{n-1} & \dots & \dots & a_0 \\ b_m & b_{m-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ 0 & b_m & \dots & \dots & b_1 & b_0 & \dots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \dots & 0 & b_m & b_{m-1} & \dots & \dots & b_0 \end{vmatrix},$$

Коэффициенты многочлена a(x) повторены (со смещением) в первых m строках, а коэффициенты b(x) – в последующих n строках. Два полинома имеют нетривиальный общий делитель, тогда и только тогда, когда их результант равен 0.

Пусть $f(x) = x^m + a_{m-1}x^{m-1} + \dots + a_1 x + a_0$ – нормированный полином положительной степени m. **Сопровождающей матрицей** полинома f(x) называется матрица

$$A = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & 0 & \dots & 0 & -a_2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & -a_{m-1} \end{bmatrix}.$$

Матрица A в некотором смысле является «корнем» полинома f(x), то есть $A^m + a_{m-1}A^{m-1} + \dots + a_1 A + a_0 E = 0$, где E и 0, соответственно единичная и нулевая квадратные матрицы порядка m.

Функцией Мебиуса называется функция натурального аргумента со значениями во множестве {-1, 0, 1}, задаваемая по следующему правилу:

$$\mu(n) = \begin{cases} 1, & \text{при } n = 1 \\ (-1)^k, & \text{при } n \text{ равном произведению } k \text{ различных простых чисел} \\ 0, & \text{при } n, \text{ делящимся на квадрат простого числа} \end{cases}$$

Функция Мебиуса удовлетворяет соотношению:

$$\sum_{d|n}\mu(d)=\begin{cases}1 & \text{при } n=1\\ 0 & \text{при } n>1\end{cases}$$

Справедлива, так называемая, **формула обращения Мебиуса**:

Пусть h и H – две функции натурального аргумента со значениями в некоторой (аддитивной) абелевой группе. Тогда соотношение

$$\forall n\in N\ H(n)=\sum_{d|n}h(d)$$

выполняется тогда и только тогда, когда справедливо соотношение

$$\forall n\in N\ h(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)H(d)$$

При оценивании временной сложности алгоритмов бывает удобна следующая терминология. Говорят, что алгоритм, зависящий от входа n, и выполняемый за время t(n), имеет временную сложность не выше O(g(n)), если существуют такие константы C и N, что $\forall n > N\ \ t(n) \le c\ g(n)$.

Строение конечных полей

Известно, что кольца классов вычетов по простым (и только по простым) модулям являются полями. Эти поля, не имеющие собственных подполей, играют в теории полей конечной характеристики примерно ту же роль, что и поле рациональных чисел в теории полей нулевой характеристики. А именно: каждое поле конечной характеристики и, в частности, каждое конечное поле содержит в качестве подполя простое поле, изоморфное $\mathbf{Z}_p$. Для доказательства этого факта достаточно рассмотреть подгруппу, аддитивно порожденную единицей поля характеристики p. Легко видеть, что эта подгруппа содержит p элементов, и, что эти элементы образуют подполе исходного поля, изоморфное $\mathbf{Z}_p$.

Рассмотрим конечное поле F. Согласно вышеизложенному, у него есть подполе из p элементов, где p – некоторое простое число. Посмотрим на F как на векторное пространство над своим простым подполем. Пусть m – размерность этого пространства и $u_1, u_2,\ldots,u_m$ – базис этого пространства. Тогда каждый элемент F единственным образом представляется в виде $c_1u_1 + c_2u_2 + \ldots + c_mu_m$, где c_i берутся из простого подполя. Ясно, что таких наборов существует ровно p^m.

Таким образом, в каждом конечном поле число элементов есть натуральная степень некоторого простого числа p. С другой стороны, для каждого простого числа p и натурального числа m существует, причем с точностью до изоморфизма ровно одно, поле из p^m элементов.

Для доказательства рассмотрим многочлен $g(x) = x^{p^m} - x$ над полем Z_p. Согласно общей теории полей, существует поле разложения полинома g(x) расширение Z_p, над которым g разлагается на линейные множители. Производная g равна -1 (напомним, что мы имеем дело с полем характеристики p), поэтому все его корни различны. Значит, поле разложения g содержит по крайней мере p^m элементов (корней g). Покажем, что эти корни уже сами по себе образуют поле. Поскольку корни g лежат в некотором поле и элементы 0 и 1 очевидно являются корнями g достаточно показать, что во множестве корней выполнимы четыре арифметических действия. Пусть α и β – корни g. Тогда:

$$(\alpha\beta)^{p^m} - \alpha\beta = \alpha^{p^m}\beta^{p^m} - \alpha\beta^{p^m} + \alpha\beta^{p^m} - \alpha\beta = (\alpha^{p^m} - \alpha)\beta^{p^m} + \alpha(\beta^{p^m} - \beta) = 0$$

и, следовательно, произведение корней g тоже является его корнем;

$$((\alpha^{-1})^{p^m} - \alpha^{-1})\alpha^{p^m+1} = \alpha - \alpha^{p^m} = 0$$

и, значит, элемент, обратный к корню *g* сам является его корнем;

$$(\alpha \pm \beta)^{p^m} - (\alpha \pm \beta) = \alpha^{p^m} \pm \beta^{p^m} - \alpha \pm \beta = (\alpha^{p^m} - \alpha) \pm (\beta^{p^m} - \beta) = 0$$

и, значит, сумма и разность корней *g* – снова его корни.

При доказательстве мы использовали тождество $(\alpha \pm \beta)^{p^m} = \alpha^{p^m} \pm \beta^{p^m}$, справедливое для полей характеристики p. При p=1 это тождество вытекает из того, что все биномиальные коэффициенты в разложении $(\alpha \pm \beta)^p$, за исключением первого и последнего будут кратны p. Для остальных m оно легко доказывается по индукции.

Итак, мы уже доказали существование поля из p^m элементов. Пусть теперь F такое поле. Порядок мультипликативной группы F равен p^m-1. Поэтому всякий ненулевой элемент α удовлетворяет соотношению $\alpha^{p^m} = \alpha$, и, значит, является корнем многочлена *g*. Ноль, очевидно, тоже является корнем этого многочлена. Следовательно поле F является полем разложения *g* над Z_p. Единственность поля из p^m элементов следует теперь из единственности (с точностью до изоморфизма) поля разложения.

Подведем итоги предыдущих рассуждений, сформулировав теорему и два следствия:

Теорема 1 (существования и единственности конечных полей)

Для каждого простого числа p и каждого натурального числа m существует поле из p^m элементов. Любое конечное поле содержит p^m элементов для подходящих p и m. Любые два поля из одного и того же числа элементов изоморфны. □

Следствие 2

В поле характеристики p справедливо тождество $(\alpha \pm \beta)^{p^m} = \alpha^{p^m} \pm \beta^{p^m}$ □

Следствие 3

В поле из p^m элементов справедливо тождество $\alpha^{p^m} = \alpha$. □

Введем обозначения, которых будем придерживаться в дальнейшем, если иное не оговорено особо. Обозначим $q = p^m$, а единственное с точностью до изоморфизма поле из q элементов обозначим через F_q.

Заметим, что к доказательству существования поля из q элементов можно было подойти по-иному. Если f(x) –многочлен m-й степени, неприводимый над полем Z_p. Тогда простое алгебраическое расширение $Z_p(\alpha)$ (где α – некоторый корень f) будет иметь степень m над Z_p и, следовательно, будет полем из q элементов. Однако на данной стадии мы еще не можем гарантировать для каждого простого p существование многочленов любой степени, неприводимых над Z_p.

Теорема 4

Мультипликативная группа конечного поля – циклическая.

Поскольку для поля из двух элементов утверждение теоремы очевидно, мы можем полагать, что q > 2. Пусть $r = q - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$.

Многочлены $h_i(x) = x^{r/p_i} - 1$ (здесь $i \in \{1,2,..,k\}$) имеют менее r корней, поэтому для каждого i в F_q есть ненулевой элемент a_i, не являющиеся корнем h_i. Пусть $b_i = a_i^{r/p_i^{\alpha_i}}$. Тогда $b_i^{p_i^{\alpha_i}} = a_i^r = 1$. Поэтому порядок b_i есть степень простого числа p_i. Но $b_i^{p_1^{\alpha_i - 1}} = a_i^{r/p_i} \neq 1$, поскольку элемент a_i не является корнем многочлена h_i. Следовательно, порядок b_i равен $p_i^{\alpha_i}$. Покажем, что элемент $g = b_1 b_2 \ldots b_k$ имеет порядок r. Ясно, $g^r = 1$. Допустим, что порядок g – собственный делитель числа r, тогда он является делителем числа r/p_i хотя бы для одного i. Не теряя общности можно считать, что i=1. Тогда $1 = g^{r/p_1} = b_1^{r/p_1} b_2^{r/p_1} \ldots b_k^{r/p_1} = b_1^{r/p_1}$, так как r/p_1 кратно порядкам остальных b_i. Но r/p_1 не кратно порядку b_1 и мы к противоречию, и, следовательно, g – порождающий элемент мультипликативной группы поля F_q. □

Замечание: На самом деле, справедливо несколько более сильное утверждение, а именно, что циклической является всякая конеч-

ная подгруппа мультипликативной группы поля (конечность самого поля не требуется).

Ранее мы отмечали, пока не можем гарантировать существование неприводимых над Z_p многочленов любых натуральных степеней. Доказанная цикличность группы F_q дает нам такую возможность.

Следствие 5

Для любого натурального числа m и любого простого числа p существует неприводимый над полем Z_p многочлен m-й степени.

Согласно теореме 1 существует поле из p^m элементов. На основании теоремы 4 в этом поле есть элемент g порядка p^m-1. Поскольку g – алгебраический элемент над Z_p у него есть минимальный неприводимый многочлен f с коэффициентами из Z_p. Поскольку g лежит в расширении поля Z_p, имеющем степень m, степень f не может быть больше m. С другой стороны, если бы степень многочлена f была меньше m, простое алгебраическое расширение $Z_p(g)$ содержало бы не более p^{m-1} элементов и g, не мог бы мультипликативно порождать группу из p^m-1 элементов. □

Заметим, что для случая m=p=2 существует всего один неприводимый многочлен – x^2+x+1. В дальнейшем мы выведем общую формулу для количества многочленов неприводимых над произвольным конечным полем F_q.

Конечные поля имеют структуру подполей, характеризующуюся решеткой натуральных делителей числа m.

Теорема 6

Для каждого натурального делителя d числа m в поле F_q существует ровно одно подполе из p^d элементов. Обратно, всякое подполе поля F_q состоит из p^d элементов, где d|m.

Пусть d|m. Тогда p^d-1|p^m-1 и $x^{p^d-1}-1 \mid x^{p^m-1}-1$. Следовательно, $x^{p^d}-x \mid x^{p^m}-x$. Значит, множество корней многочлена $x^{p^d}-x$, образующих, как было доказано ранее, поле из p^d элементов, является подмножеством и подполем поля F_q.

Обратно, если E – подполе поля F_q, то оно, являясь расширением Z_p, обязано содержать p^d элементов (для некоторого натурального числа d). В то же время, число элементов F_q, являющегося векторным пространством над E, должно быть степенью p^d и, следовательно, d обязано быть делителем m.

Наконец, F_q не может содержать более одного подполя из p^d элементов, так как в противном случае многочлен $x^{p^d}-x$ имел бы более p^d корней в поле F_q. □

Мы видели, что все элементы конечного поля представляют собой корни одного и того же многочлена – $x^{p^m}-x$. Этот многочлен,

очевидно, приводим. В то же время, как известно из курса алгебры, для каждого элемента, алгебраического над некоторым полем (а в конечном поле все элементы, разумеется, алгебраичны над любым подполем), существует минимальный неприводимый многочлен. Оказывается, каждое конечное поле представляет собой объединение множеств корней некоторого множества полиномов, неприводимых над произвольным фиксированным подполем исходного поля.

Лемма 7

Возведение в p-ю степень является автоморфизмом поля F_q.

Пусть σ – отображение F_q в себя, действующее по правилу: $\sigma(\alpha) = \alpha^p$. В силу следствия 2 и очевидного факта, что произведение p-х степеней есть p-я степень произведения, остается доказать лишь биективность σ. А ввиду конечности F_q для этого достаточно убедиться в инъективности σ. Но инъективность σ очевидна, поскольку F_q, являясь полем, не содержит делителей нуля и, значит, ядро гомоморфизма σ состоит только из нуля. □

Лемма 8

Многочлен, неприводимый над конечным полем, не имеет кратных корней.

Пусть f(x) – многочлен, неприводимый над F_q. Если у f есть кратные корни, то он обязан иметь нетривиальный НОД со своей производной. Поскольку f неприводим, единственной возможностью остается обращение f’ в нуль. Это, в свою очередь, возможно лишь в том случае, когда все коэффициенты многочлена f при степенях не кратных p равны нулю и f имеет вид: $\sum_{i=0}^{d} a_i x^{ip}$. В силу леммы 7, каждое a_i равно некоторому b_i^p. Учитывая следствие 2, получим $f(x) = \left(\sum_{i=0}^{d} b_i x^i\right)^p$. Таким образом, многочлен f является p-й степенью некоторого многочлена над полем F_q и не может быть неприводимым. □

Лемма 9

Пусть f(x) – неприводимый над F_q многочлен степени d. Тогда f(x) делит полином $x^{q^n} - x$ в том и только в том случае, когда d|n.

Пусть сначала $f(x) \mid x^{q^n} - x$ и пусть α – некоторый корень f(x). Тогда $\alpha^{q^n} = \alpha$ и, значит, $\alpha \in F_{q^n}$. Но тогда простое алгебраическое расширение $F_q(\alpha)$ имеет степень d над F_q и является подполем F_{q^n},

которое, в свою очередь, имеет степень n над F_q. Следовательно, на основании теоремы о башне расширений можно заключить, что d|n.

Обратно, пусть d|n. Тогда простое алгебраическое расширение $F_q(\alpha)$ содержит q^d элементов. На основании теорем 1 и 6 множество корней многочлена $x^{q^n} - x$, являясь полем из q^n элементов, содержит подполе из q^d элементов, изоморфное $F_q(\alpha)$. Следовательно, α удовлетворяет соотношению $\alpha^{q^n} = \alpha$, то есть является корнем полинома $x^{q^n} - x$. Но тогда $f(x) \mid x^{q^n} - x$. □

Лемма 10

Если хотя бы один корень неприводимого над F_q многочлена f лежит в некотором расширении поля F_q, то и все его корни лежат в этом расширении. Причем эти корни получаются последовательным возведением в q-ю степень любого из них.

Пусть $f(x) = \sum_{i=0}^{d} a_i x^i$ – многочлен, неприводимый над F_q, и α – корень этого многочлена, лежащий в некотором расширении поля F_q. Используя следствия 2 и 3, непосредственной проверкой убеждаемся, что α^q также будет корнем f. Действительно, $f(\alpha^q) = \sum_{i=0}^{d} a_i \alpha^{qi} = \sum_{i=0}^{d} a_i^q \alpha^{iq} = \left(\sum_{i=0}^{d} a_i \alpha^i\right)^q = 0^q = 0$.

Для доказательства утверждения леммы остается проверить, что среди элементов α^{q^k} ровно d будут различными. Пусть это не так. Тогда $\alpha^{q^i} = \alpha^{q^j}$ для некоторых i и j таких, что $0 \le i < j < d$. Если возвести обе части этого равенства в степень q^{d-j}, получим $\alpha^{q^{d-j+i}} = \alpha^{q^d} = \alpha$ (последнее соотношение следует из того, что α лежит в поле $F_q(\alpha)$, содержащем q^d элементов). Значит , α - корень многочлена $x^{q^{d-j+i}} - x$. Но тогда, согласно лемме 9 степень f(x) должна делить число d-j+i, что, очевидно, невозможно. □

Мы знаем, что все элементы поля F_q являются корнями одного многочлена $g(x) = x^q - x$. Из доказанных лемм 9 и 10 вытекает еще одна характеризация элементов конечного поля:

Теорема 11

Пусть F_{q^n} конечное поле. Тогда оно состоит из всех корней всех неприводимых над F_q полиномов, степени которых есть делители числа n. Все корни этих полиномов просты и получаются друг из друга последовательным возведением в q-ю степень. □

Мы видели, что возведение в p-ю степень является автоморфизмом конечного поля характеристики p. Такой автоморфизм оставля-

ет на месте элементы простого подполя и переставляет остальные элементы (они переходят в другие корни минимальных неприводимых над Z_p полиномов для этих элементов). Аналогичная ситуация получается, если рассматривать возведение q-ю степень в поле F_{q^n}. Такой автоморфизм (обозначим его σ) будет оставлять на месте элементы поля F_q, являющиеся корнями неприводимых над F_q полиномов первой степени, и переводить остальные элементы в другие корни их неприводимых над F_q полиномов.

С другой стороны, каждый автоморфизм δ поля F_{q^n} над F_q должен, очевидно, переводить корень α неприводимого над F_q полинома f(x) в корень того же полинома. Следовательно, $\delta(\alpha) = \alpha^{q^k}$, для некоторого натурального k, не превосходящего n. Если f(x) имеет степень n, то элементы 1, α, α^2, α^{n-1} образуют базис F_{q^n} над F_q. Раскладывая произвольный элемент β поля F_{q^n} по этому базису, учитывая сохранение операций при автоморфизме, и, применяя следствие 2, убедимся, что , $\delta(\alpha) = \alpha^{q^k}$. Таким образом каждый автоморфизм поля F_{q^n} над F_q некоторая степень автоморфизма σ. Автоморфизм σ называют автоморфизмом Фробениуса.

В случае конечных полей любое поле, очевидно, нормально и сепарабельно над любым своим подполем. Из приведенных выше рассуждений видно, группа Галуа конечного поля над любым своим подполем устроена максимально просто. А именно имеет место

Теорема 12

Группа Галуа поля F_{q^n} над полем F_q является циклической группой n-го порядка, порожденной автоморфизмом Фробениуса. □

Элементы расширения E поля F называются сопряженными над F, если они являются корнями одного и того же неприводимого над F полинома. (Например, комплексно-сопряженные числа являются корнями одного и того же квадратного уравнения с коэффициентами из **R**. В случае расширения F_{q^n} поля F_q сопряженные над F_q элементы получаются последовательным возведением любого из них в q-ю степень. Таким образом, возведение в q-ю степень задает на множестве элементов F_{q^n} структуру унара, каждая компонента связности которого представляет собой цикл, длина которого – делитель числа n. Количество циклов длины d есть количество нормированных (т. е. имеющих старшим коэффициентом единицу) неприводимых над F_q многочленов степени d. Обозначим это число через $N_q(d)$.

Выведем явную формулу для нахождения $N_q(d)$.

Теорема 13

$$N_q(n) = \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d$$

На основании теоремы 11 имеем $q^n = \sum_{d|n} d\,N_q(d)$. Требуемый результат получается применением к этому равенству формулы обращения Мебиуса, если положить: $H(n) = q^n$, $h(n) = n \cdot N_q(n)$. □

Представление элементов конечных полей

Наиболее простое (а зачастую и наиболее удобное) представление элементов конечного поля получается при рассмотрении этого поля как простого алгебраического расширения своего простого подполя. Для того, чтобы воспользоваться этим способом представления элементов поля F_q, нам потребуется неприводимый над Z_p полином m-й степени (к вопросу как найти такой полином мы вернемся позже). Пусть f(x) – такой полином, а α – его какой-либо корень (на самом деле это просто класс многочлена x в факторкольце $Z_p/(f(x))$. Тогда элементы 1, α, α^2,…α^{m-1} образуют базис F_q как векторного пространства над Z_p. Поэтому всякий элемент F_q единственным образом представляется в виде линейной комбинации $c_0 + c_1\alpha + c_2\alpha^2 +\ldots+ c_{m-1}\alpha^{m-1}$, с коэффициентами из Z_p. Элементы из F_q складываются как векторы, а перемножаются как многочлены с последующим приведением результата по модулю полинома f(x) (иными словами, результат умножения заменяется своим остатком от деления на f). Разумеется, все операции над коэффициентами производятся по модулю p.

Возведение в натуральную степень, разумеется, может быть сведено к последовательному умножению. Однако, если показатель степени велик, последовательное домножение на возводимый элемент будет очень неэффективно. Гораздо лучший (по временным затратам) результат даст бинарный алгоритм возведения в степень.

Итак, пусть α – элемент и k – натуральный показатель степени, в которую надо возвести α. Выполним начальные присвоения u:=α, v:=1. Пусть $k = a_0 + 2a_1 +2^2a_2 +\ldots+ 2^sa_s$, где каждое a_i есть 0 или 1. Тогда $\alpha^k = \prod_{i=0}^{s}\alpha^{2^i a_i}$. Из этой формулы ясно, что для нахождения α^k достаточно Повторить в цикле (i изменяется от 0 до s) следующие действия:

1) Если a_i не равно 0, v:=v*u;
2) u:=u*u.

Заметим, что приведенный алгоритм применим для нахождения k-той степени, элементов любых множеств, в которых задана ассоциативная операция умножения, а не только для конечных полей.

Для реализации деления достаточно уметь находить обратный к данному ненулевому элементу. Сделать это можно несколькими путями.

Первый из этих подходов является универсальным для любых простых алгебраических расширений (и даже для любых евклидовых колец). Если $c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_{m-1}\alpha^{m-1}$ – ненулевой элемент поля F_q, то многочлены $h(x) = c_0 + c_1x + c_2x^2 + \ldots + c_{m-1}x^{m-1}$ и $f(x)$ взаимно просты. Потому единица представляется в виде их линейной комбинации, причем коэффициенты в линейном выражении единицы можно эффективно найти с помощью алгоритма Евклида. Пусть $s(x)$ – коэффициент при $h(x)$, тогда $s(\alpha)$ и есть искомый обратный элемент.

Второй подход существенно опирается на конечность поля F_q. Поскольку мультипликативная группа поля F_q содержит q-1 элемент, для всякого ненулевого элемента β выполняется соотношение $\beta^{q-1} = \beta$, и, следовательно, элемент β^{q-2} является обратным к β. Может показаться, что этот метод гораздо более трудоемок, чем предыдущий. Однако, применение бинарного алгоритма возведения в степень позволяет получить ответ за время $O(\log q)$.

В некоторых случаях вместо полиномиального базиса эффективнее использовать, так называемый, нормальный базис. Нормальным базисом расширения F_{q^n} поля F_q называется базис, образованный сопряженными над F_q элементами $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$. В частности, нормальный базис поля F_q над Z_p имеет вид: $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{m-1}}$. Разумеется, не для любого элемента α приведенная система будет базисом. Так, если степень d минимального неприводимого полинома для α является собственным делителем числа m, то среди элементов $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ будут повторяющиеся. Но даже если степень минимального неприводимого полинома элемента α равна m это вовсе не гарантия того, что элементы $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ будут линейно независимы. Однако справедливы следующие утверждения, которые мы приведем без доказательства:

Теорема 14

Для каждого конечного расширения F_{q^n} конечного поля F_q существует нормальный базис F_{q^n} над F_q. □

Теорема 15

Следующие условия равносильны:

1) *Система* $\alpha,\alpha^{q},\alpha^{q^2},\ldots,\alpha^{q^{n-1}}$ *является базисом* F_{q^n} *над* F_q*;*

2) *Детерминант* $\begin{vmatrix} \alpha & \alpha^{q} & \alpha^{q^2} & \ldots & \alpha^{q^{n-1}} \\ \alpha^{q^{n-1}} & \alpha & \alpha^{q} & \ldots & \alpha^{q^{n-2}} \\ \alpha^{q^{n-2}} & \alpha^{q^{n-1}} & \alpha & \ldots & \alpha^{q^{n-3}} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \alpha^{q} & \alpha^{q^{q}} & \alpha^{q^{3}} & \ldots & \alpha \end{vmatrix}$ *отличен от нуля;*

3) *Полиномы* x^n-1 *и* $\alpha x^{n-1}+\alpha^{q}x^{n-2}+\ldots+\alpha^{q^{n-2}}x+\alpha^{q^{n-1}}$ *взаимно просты.* □

Отметим, что при использовании нормального базиса для представления элементов поля F_q следует заранее заготовить таблицу умножения для базисных элементов.

Следующий способ представления элементов конечного поля опирается на циклическое строение мультипликативной группы. Если b – порождающий элемент группы F_q^*, то каждый ненулевой элемент однозначно представляется в виде b^i, где $i\in\{0, 1, \ldots, q-1\}$. Умножение элементов, представленных в таком виде, производится очень удобно – сложением показателей с последующим приведением по модулю q-1. Однако, такое представление не приспособлено для сложения элементов F_q. Поэтому при использовании этого представления приходится хранить таблицу индексов для конвертирования элементов в формат векторов в некотором базисе. Альтернативный вариант – хранить таблицу для «прибавления» единицы к произвольному элементу. Сложение любых элементов F_q можно свести к умножению и этому случаю: $b^i+b^j = b^j(b^{i-j} + 1)$. Оба варианта требуют предварительных вычислений и последующего хранения q-1 элемента (вектора или числа). Понятно, что для больших q такой подход неприемлем.

Еще один способ представления элементов F_q основан на использовании сопровождающей матрицы неприводимого над Z_p полинома m-й степени. Пусть f(x) – нормированный полином положительной степени m и A – его сопровождающая матрица. Матрица A соответствует элементу α в представлении элементов F_q с помощью полиномиального базиса. Следовательно, остальные элементы поля F_q можно представить в виде многочленов от A степеней меньших m с коэффициентами из Z_p, значением которых будут в этом случае некоторые квадратные матрицы над Z_p порядка m.

Пример 16

Пусть p = 7 и m = 3. Полином $x^3 + x^2 + 2x + 4$ неприводим над $\mathbf{Z}_7$. Сопровождающая матрица этого полинома - $A = \begin{pmatrix} 0 & 0 & 3 \\ 1 & 0 & 5 \\ 0 & 1 & 6 \end{pmatrix}$ соответствует элементу α полиномиального базиса. Тогда, например, элемент $3 + \alpha$ представляется в виде $A + 3E = \begin{pmatrix} 3 & 0 & 3 \\ 1 & 3 & 5 \\ 0 & 1 & 2 \end{pmatrix}$, а элемент α^2 – в виде $A^2 = \begin{pmatrix} 1 & 3 & 4 \\ 0 & 5 & 5 \\ 1 & 6 & 6 \end{pmatrix}$.□

Преимуществом такого представления является то, что действия над элементами соответствуют обычным сложению и умножению матриц над Z_p. Недостатком же является «разреженность» такого представления. Действительно, всего существует p^{m^2} квадратных матриц над Z_p порядка m, но лишь p^m из них представляют элементы поля F_q.

Рассмотрим достаточно объемный пример, иллюстрирующий большую часть изложенного выше о конечных полях.

Пример 17

Возьмем p = 3 и m = 4. Поле F_{81} должно содержать по одному подполю из трех и девяти элементов и состоять из 3-х корней трех полиномов 1-й степени, 6-и корней трех полиномов 2-й степени и 72-х корней восемнадцати полиномов 4-й степени неприводимых над Z_p. Для представления элементов F_{81} с помощью полиномиального базиса нам понадобится один из 18 неприводимых над Z_3 полиномов 4-й степени. В дальнейшем мы изложим эффективные методы проверки полинома на неприводимость и построения неприводимых полиномов. Но в нашем случае (для небольших p и m) вполне можно подобрать подходящий полином непосредственной проверкой. Ясно, что нормированные неприводимые над Z_3 полиномы 1-й степени исчерпываются следующими: $h_0(x) = x$, $h_1(x) = x + 2$, $h_2(x) = x + 1$. Среди 9-и нормированных полиномов 2-й степени неприводимыми будут в точности те, которые не имеют корней в Z_3. Это $g_0(x) = x^2 + 1$, $g_1(x) = x^2 + x + 2$ и $g_2(x) = x^2 + 2x + 2$. Для того, чтобы многочлен 4-й степени был неприводим достаточно, чтобы он не делился ни на один из вышеперечисленных полиномов. Наиболее удобными для организации умножения в полиномиальном базисе

являются двучлены вида $x^m + a$. Однако в нашем случае все двучлены оказываются приводимы. Поэтому обратимся к трехчленам вида $x^4 + ax + b$. Непосредственной проверкой убеждаемся, что полином $f_0(x) = x^4 + 2x + 2$ неприводим. Если α корень этого полинома, то $\alpha^4 = \alpha + 1$. Это тождество во многих случаях удобнее, чем выполнение деления с остатком на $f_0(x)$.

Итак, мы имеем полиномиальный базис 1, α, α^2, α^3 и каждый элемент нашего поля однозначно представляется в виде вектора $c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3$ с коэффициентами из Z_3. В дальнейшем мы иногда будем записывать эти векторы как упорядоченные наборы координат, но в случаях, когда это способствует пониманию материала, будем придерживаться развернутой записи.

Найдем остальные корни $f_0(x)$. Напомним, что для это достаточно последовательно найти α^3, α^9, α^{27}. Имеем:

$\alpha^3 = (0, 0, 0, 1)$;

$\alpha^9 = \alpha^4\alpha^4\alpha = (1 + \alpha)^2\alpha = \alpha + 2\alpha^2 + \alpha^3 = (0, 1, 2, 1)$;

$\alpha^{27} = (\alpha + 2\alpha^2 + \alpha^3)^3 = \alpha^3 + 2\alpha^6 + \alpha^9 = \alpha^3 + 2\alpha^2(1+\alpha) + \alpha + 2\alpha^2 + \alpha^3$ $= \alpha + \alpha^2 + \alpha^3 = (0, 1, 1, 1)$.

При вычислениях мы использовали тождество $\alpha^4 = \alpha + 1$, следствие 2 и инвариантность элементов Z_p относительно возведения в p-ю степень. Мы достаточно подробно привели промежуточные выкладки. В дальнейшем мы часто будем их опускать, предоставляя читателю право воспроизвести их самостоятельно (читателю рекомендуется не пренебрегать этим правом до тех пор, пока вычисления в конечных полях не станут для него простыми и обыденными).

Итак, из 81-го элемента F_{81} 4 являются корнями $f_0(x)$. Еще 3 принадлежат полю Z_3 и являются корнями полиномов первой степени. Для того, чтобы сопоставить 76-и остальным элементам их минимальные неприводимые многочлены можно поступить, например, так. Если для некоторого элемента еще не найден его минимальный неприводимый многочлен, начнем последовательно вычислять его 3-ю, 9-ю и 27-ю степени (если 9-я степень совпадет с 1-й, то соответствующий элемент лежит в подполе F_9 и является корнем полинома 2-й степени). После нахождения всех корней очередного неприводимого полинома для вычисления его коэффициентов достаточно воспользоваться формулами Виета. Альтернативный способ нахождения минимального неприводимого полинома – метод неопределенных коэффициентов.

Прежде чем вычислять неприводимые многочлены для элементов поля F_{81} найдем порождающий элемент (его также называют первообразным корнем из единицы) мультипликативной группы поля. Мы также составим таблицу степеней первообразного корня, со-

поставив каждому элементу его индекс – наименьший натуральный показатель степени, в которую надо возвести первообразный корень, чтобы получить данный элемент. Эта таблица будет полезна для нахождения элементов, сопряженных с данным. Поскольку мультипликативная группа поля F_{81}^* содержит $\varphi(80) = 32$ первообразных корня, то подходящий элемент можно отыскать методом проб. При этом для проверки того, является ли элемент первообразным корнем, нет нужды вычислять все его степени подряд. Учитывая, что 80 имеет всего два простых делителя, заключаем, что всякий элемент, не являющийся первообразным корнем, должен давать единицу при возведении его в 16-ю либо 40-ю степень. Начнем проверку с α. Имеем:

$\alpha^{16} = \left(\alpha^4\right)^4 = (1+\alpha)^4 = 2 + 2\alpha + \alpha^3$:

$\alpha^{40} = \left(\alpha^{16} \cdot \alpha^4\right)^2 = ((2 + 2\alpha + \alpha^3)(1+\alpha))^2 = 2.$

Таким образом, α является первообразным корнем. Ясно, что остальные первообразные корни соответствуют степеням α, взаимно простым с 80. Таблица степеней α приведена ниже.

Используя таблицу степеней первообразного корня, легко найти элементы, принадлежащие подполю F_9 и их минимальные неприводимые полиномы. Ненулевые элементы из F_9 должны образовывать восьмиэлементную подгруппу группы F_{81}^*. Ясно, что это элементы с индексами, кратными 10. Два из таких элементов (с индексами 40 и 80) принадлежат полю Z_3, а остальные шесть должны разбиваться на три группы по два элемента, переходящих в друг друга при возведении в куб. Несложные расчеты по модулю 80 показывают, что одну из этих групп составляют элементы с индексами 20 и 60, другую – элементы с индексами 10 и 30, а третью – элементы с индексами 50 и 70. Применяя формулы Виета, находим, что неприводимыми полиномами для этих пар элементов являются соответственно $g_0(x)$, $g_1(x)$ и $g_2(x)$.

Найдем сопряженные элементы и минимальный неприводимый полином, например, для элемента $\beta = 1 + \alpha$. Имеем:

$\beta^3 = (1 + \alpha)^3 = 1 + \alpha^3$;

$\beta^9 = (1 + \alpha)^9 = 1 + \alpha + 2\alpha^2 + \alpha^3$;

$\beta^{27} = (1+\alpha)^{27} = 1 + \alpha + \alpha^2 + \alpha^3$.

Пусть $f_1(x) = x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$ – неприводимый полином для β. По формулам Виета находим $b_3 = -(\beta + \beta^3 + \beta^9 + \beta^{27}) = 2$ и $b_0 = \beta^{40} = (1 + \alpha)^{160} = 1$. Чтобы не вычислять громоздкие выражения для b_1 и b_2 найдем эти коэффициенты методом неопределенных коэффи-

циентов, подставив $1 + \alpha$ вместо x в $f_1(x)$ и приравняв полученное выражение к 0:

$(1 +\alpha)^4 + 2(1 + \alpha)^3 + b_2(1 + \alpha)^2 + b_1(1+\alpha) + 1 = 0.$

Раскрывая скобки и приравнивая коэффициенты при одинаковых степенях α к нулю, находим: $b_1 = 1$, $b_2 = 0$. Окончательно имеем: $f_1(x) = x^4 + 2x^3 + x + 1$.

Можно заметить, что все четыре корня полинома $f_1(x)$, рассматриваемые как многочлены от α, имеют одинаковый свободный член. Такая же картина, имеет место и для корней полиномов $f_0(x)$ и $g_i(x)$. Этот факт не случаен. Пусть $\beta = c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3$. Тогда $\beta^3 = c_0 + c_1\alpha^3 + c_2(1 + \alpha)\alpha^2 + c_3(1 + \alpha)^2\alpha$. Таким образом, сопряженные элементы имеют одинаковые свободные члены в разложении по полиномиальному базису.

Заметим также, что если к сопряженным между собой элементам прибавить одну и ту же константу из Z_3, то вновь полученные элементы тоже будут сопряжены между собой. Это следует из тождества $(\beta + c)^3 = \beta^3 + c$, где β – произвольный элемент поля F_{81}, а c берется из Z_3.

Приведенные выше соображения позволяют значительно упростить сопоставление элементам F_{81} их неприводимых полиномов. Перечислим остальные неприводимые над Z_3 полиномы 4-й степени:

$f_2(x) = x^4 + x^3 + 2;$

$f_3(x) = x^4 + x^2 + 2x + 1;$

$f_4(x) = x^4 + 2x^3 + x^2 + 2x + 1;$

$f_5(x) = x^4 + x^3 + x^2 + 2x + 2;$

$f_6(x) = x^4 + x^2 + 2;$

$f_7(x) = x^4\, 2x^3 + x^2 + 1;$

$f_8(x) = x^4 + x^3 + x^2 + 1;$

$f_9(x) = x^4 + 2x^2 + 2;$

$f_{10}(x) = x^4 + 2x^3 + 2x^2 + x + 2;$

$f_{11}(x) = x^4 + x^3 + 2x^2 + 2x + 2;$

$f_{12}(x) = x^4 + x + 2;$

$f_{13}(x) = x^4 + 2x^3 + 2;$

$f_{14}(x) = x^4 + x^3 + 2x + 1;$

$f_{15}(x) = x^4 + x^2 + x + 1;$

$f_{16}(x) = x^4 + 2x^3 + x^2 + x + 2;$

$f_{17}(x) = x^4 + x^3 + x^2 + x + 1.$

Занесем результаты предыдущих вычислений в таблицу, сопоставив каждому элементу поля F_{81} его индекс и неприводимый полином, корнем которого является этот элемент.

Таблица 18

Элемент	Индекс	Полином
α	1	f_0
α^2	2	f_5
α^3	3	f_0
$1+\alpha$	4	f_1
$\alpha+\alpha^2$	5	f_6
$\alpha^2+\alpha^3$	6	f_3
$1+\alpha+\alpha^3$	7	f_{10}
$1+2\alpha+\alpha^2$	8	f_4
$\alpha+2\alpha^2+\alpha^3$	9	f_0
$1+\alpha+\alpha^2+2\alpha^3$	10	g_1
$2+\alpha^2+\alpha^3$	11	f_5
$1+\alpha^3$	12	f_1
$1+2\alpha$	13	f_{13}
$\alpha+2\alpha^2$	14	f_{15}
$\alpha^2+2\alpha^3$	15	f_6
$2+2\alpha+\alpha^3$	16	f_{17}
$1+2\alpha^2$	17	f_{16}
$\alpha+2\alpha^3$	18	f_3
$2+2\alpha+\alpha^2$	19	f_5
$2\alpha+2\alpha^2+\alpha^3$	20	g_0
$1+\alpha+2\alpha^2+2\alpha^3$	21	f_{10}
$2+\alpha^2+2\alpha^3$	22	f_8
$2+\alpha+\alpha^3$	23	f_{11}
$1+\alpha^2$	24	f_4
$\alpha+\alpha^3$	25	f_9
$1+\alpha+\alpha^2$	26	f_7
$\alpha+\alpha^2+\alpha^3$	27	f_0
$1+\alpha+\alpha^2+\alpha^3$	28	f_1
$1+2\alpha+\alpha^2+\alpha^3$	29	f_{10}
$1+2\alpha+2\alpha^2+\alpha^3$	30	g_1

Элемент	Индекс	Полином
2α	41	f_{12}
$2\alpha^2$	42	f_{15}
$2\alpha^3$	43	f_{12}
$2+2\alpha$	44	f_{14}
$2\alpha+2\alpha^2$	45	f_6
$2\alpha^2+2\alpha^3$	46	f_{15}
$2+2\alpha+2\alpha^3$	47	f_{11}
$2+\alpha+\alpha^2$	48	f_{17}
$2\alpha+\alpha^2+2\alpha^3$	49	f_{12}
$2+2\alpha+2\alpha^2+\alpha^3$	50	g_2
$1+2\alpha^2+2\alpha^3$	51	f_{16}
$2+2\alpha^3$	52	f_{14}
$2+\alpha$	53	f_2
$2\alpha+\alpha^2$	54	f_3
$2\alpha^2+\alpha^3$	55	f_6
$1+\alpha+2\alpha^3$	56	f_{14}
$2+\alpha^2$	57	f_5
$2\alpha+\alpha^3$	58	f_{15}
$1+\alpha+2\alpha^2$	59	f_{16}
$\alpha+\alpha^2+2\alpha^3$	60	g_0
$2+2\alpha+\alpha^2+\alpha^3$	61	f_{11}
$1+2\alpha^2+\alpha^3$	62	f_7
$1+2\alpha+2\alpha^3$	63	f_{10}
$2+2\alpha^2$	64	f_{17}
$2\alpha+2\alpha^3$	65	f_9
$2+2\alpha+2\alpha^2$	66	f_8
$2\alpha+2\alpha^2+2\alpha^3$	67	f_{12}
$2+2\alpha+2\alpha^2+2\alpha^3$	68	f_{14}
$2+\alpha+2\alpha^2+2\alpha^3$	69	f_{11}
$2+\alpha+\alpha^2+2\alpha^3$	70	g_2

Элемент	Индекс	Полином
$1+2\alpha+2\alpha^2+2\alpha^3$	31	f_{13}
$2+2\alpha^2+2\alpha^3$	32	f_{17}
$2+\alpha+2\alpha^3$	33	f_5
$2+\alpha+\alpha^2$	34	f_8
$2\alpha+\alpha^2+\alpha^3$	35	f_9
$1+\alpha+2\alpha^2+\alpha^3$	36	f_1
$1+2\alpha+\alpha^2+2\alpha^3$	37	f_{13}
$2+2\alpha^2+\alpha^3$	38	f_8
$1+2\alpha^3$	39	f_{13}
2	40	h_2

Элемент	Индекс	Полином
$2+\alpha+\alpha^2+\alpha^3$	71	f_2
$1+\alpha^2+\alpha^3$	72	f_4
$1+2\alpha+\alpha^3$	73	f_{16}
$1+2\alpha+2\alpha^2$	74	f_7
$\alpha+2\alpha^2+2\alpha^3$	75	f_9
$2+2\alpha+\alpha^2+2\alpha^3$	76	f_{14}
$2+\alpha+2\alpha^2+\alpha^3$	77	f_2
$1+\alpha^2+2\alpha^3$	78	f_7
$2+\alpha^3$	79	f_2
1	80	h_1
0	–	h_0

Поле F_{81} можно рассматривать не только как расширение 4-й степени поля Z_3, но и как квадратичное расширение поля F_9. Ясно, что над F_9 полиномы $g_0(x)$, $g_1(x)$, $g_2(x)$ распадутся на линейные множители, а полиномы $f_0(x)$, $f_1(x)$, ..., $f_{17}(x)$ – на неприводимые множители второй степени. Разложим, например, полином $f_0(x)$. Обозначим корень полинома g_0 $2\alpha+2\alpha^2+\alpha^3 = \beta$. Тогда второй корень g_0 будет равен 2β. Элементы поля F_9 могут быть представлены в виде линейных комбинаций базисных элементов 1 и β с коэффициентами из Z_3. Четыре корня полинома $f_0(x)$ естественным образом разбиваются на две пары так, что элементы одной пары получаются друг из друга возведением в 9-ю степень (такое возведение является единственным нетривиальным автоморфизмом F_{81} над F_9). Коэффициенты разложения $f_0(x)$ над F_9 найдем, применяя формулы Виета:

$-(\alpha + \alpha^9) = \alpha + \alpha^2 + 2\alpha^3 = 2\beta$; $\alpha\alpha^9 = 1+2\beta$;

$-(\alpha^3+\alpha^{27}) = 2\alpha + 2\alpha^2 +\alpha^3 = \beta$; $\alpha^3\alpha^{27} = 1+2\beta$.

Таким образом, $f_0(x) = (x^2 + 2\beta x + 1 + \beta)(x^2 + \beta x + 1 + \beta)$. □

Факторизация многочленов над конечными полями

В примере рассмотренном в конце предыдущего параграфа нам удалось разложить многочлен на неприводимые множители над полем F_9. Процесс разложения не потребовал от нас больших вычислений, поскольку заранее знали корни разлагаемого многочлена. Зададимся теперь целью научиться факторизовать многочлены над конечными полями в менее комфортной ситуации, когда заранее не известны ни корни многочлена, ни структура разложения.

Прежде всего мы покажем, что проблема может быть сведена к случаю разложения многочлена, не имеющего кратных множителей.

В самом деле, пусть g(x) некоторый многочлен над F_q и (неизвестное пока нам) каноническое разложение g(x) над F_q имеет вид: $g(x) = f_1^{k_1}(x) f_2^{k_2}(x) .. f_s^{k_s}(x)$. Для отделения кратных множителей f найдем его формальную производную:

$$g'(x) = k_1 f_1^{k_1-1}(x) f_1'(x) f_2^{k_2}(x) ... f_s^{k_s}(x) + ... + k_s f_1^{k_1}(x) f_2^{k_2}(x) ... f_s^{k_s-1} f_s'(x) \quad (1)$$

Некоторые из слагаемых в правой части (1) могут оказаться равны нулю. Это произойдет с теми слагаемыми, коэффициенты при которых кратны p.

Рассмотрим сначала случай, когда g`(x) полностью обратится в нуль. Это возможно в том и только в том случае, когда сам g(x) является p-й степенью, некоторого многочлена с коэффициентами из F_q. При доказательстве леммы 8 мы уже рассматривали такую ситуацию. Для явного нахождения коэффициентов многочлена t(x) такого, что $g(x) = (t(x))^p$ удобно иметь таблицу индексов. Тогда извлечение корней p-й степени из коэффициентов g(x) сведется к решению линейных сравнений вида $pz \equiv ind(a_i) (mod\ q-1)$ относительно переменной z. Можно составить и другую таблицу, в которой непосредственно для каждого элемента будет указан корень p-й степени из него. (Заметим, что если коэффициенты f(x) принадлежат Z_p, никаких таблиц не понадобится, поскольку каждый элемент Z_p совпадает со своей p-й степенью.) Ясно, что составление и хранение таблиц возможно лишь для случая относительно небольших q. Особенности разложения многочленов над большими конечными полями мы обсудим ниже.

Итак, если g`(x) = 0, мы можем свести задачу к разложению нового многочлена, степень которого в p раз меньше степени исходного. Повторяя, если надо, этот процесс, придем к многочлену с ненулевой производной. Поэтому, не нарушая общности рассуждений, мы можем считать, что $g`(x) \neq 0$. Из (1) видно, что неприводимые множители $f_i(x)$ многочлена g(x), показатели степени которых кратны p, входят в разложение g`(x) в той же степени, что и в разложение g(x). Показатели степени остальных множителей $f_i(x)$ в разложении будут на единицу меньше, чем их показатели в разложении g(x). Отсюда видно, что многочлен f(x) = g(x)/(g(x), g'(x)) будет равен произведению первых степеней различных простых сомножителей $f_i(x)$ многочлена g(x), для которых k_i не кратно p.

Прежде чем приступать к факторизации многочлена f(x), отвечающего условию отсутствия кратных множителей, покажем, как, зная разложение f(x), найти разложение g(x). Понятно, что для этого надо факторизовать (g(x), g`(x)). Для этого, прежде всего, поделим (g(x), g`(x)) на каждый из найденных неприводимых делителей f(x) столько раз, сколько такое деление окажется возможным. Тем са-

мым мы найдем показатели k_i для тех неприводимых множителей $f_i(x)$, для которых эти показатели не кратны k. Если после всех таких делений от многочлена (g(x), g`(x)) останется нетривиальное частное, то оно, очевидно, будет содержать лишь неприводимые сомножители исходного многочлена, входящие в его разложение в степенях кратных p. Такое частное будет p-й, степенью, а как поступать в этом случае, мы уже знаем. Поскольку, в результате наших манипуляций, степень многочлена, подлежащего факторизации уменьшается, то за конечное число шагов мы придем к разложению исходного многочлена.

Итак, нам осталось научиться раскладывать на множители многочлен f(x), не имеющий кратных множителей. Для построения и обоснования алгоритма факторизации таких многочленов нам, прежде всего, потребуется:

Лемма 19

$$h(x)^q - h(x) = \prod_{c \in F_q} (h(x) - c)$$

Мы знаем, что поле F_q состоит из всех корней многочлена $x^q - x$, т.е. имеет место тождество: $x^q - x = \prod_{c \in F_q} (x - c)$. Утверждение леммы получается подстановкой в это тождество h(x) вместо x. □

Основную роль в конструировании открытого Берлекэмпом алгоритма факторизации над конечным полем многочленов, не имеющих кратных множителей, играет следующая теорема:

Теорема 20

Пусть f(x) и h(x) многочлены из кольца $F_q[x]$, причем f (x) – нормирован. Тогда, если h(x) удовлетворяет сравнению

$$h(x)^q \equiv h(x) \pmod{f(x)}, \quad (2)$$

то

$$f(x) = \prod_{c \in F_q} (f(x), h(x) - c) \quad (3)$$

По условию f(x) делит $h(x)^q - h(x)$, следовательно, f(x) = (f(x), $h(x)^q - h(x)$). Отсюда, в силу леммы 19, $f(x) = (f(x), \prod_{c \in F_q} (h(x) - c))$. Учитывая, что при различных c многочлены h(x) – c попарно взаимно просты окончательно получаем: $f(x) = \prod_{c \in F_q} (f(x), h(x) - c)$. □

Заметим, что разложение (3) может оказаться и тривиальным. Так, если $h(x) \equiv c \pmod{f(x)}$, то условие теоремы 20 для него, очевидно, выполнено: $h^q(x) \equiv c^q = c \equiv h(x) \pmod{f(x)}$. Но в этом случае,

один из сомножителей произведения $\prod_{c\in F_q}(f(x),h(x)-c)$ будет равен f(x), а остальные равны единице.

Однако, если $0 < \deg(h(x)) < \deg(f(x))$, то разложение (3) уже не может быть тривиальным, поскольку степени всех сомножителей в правой части равенства (3) в этом случае будут меньше степени f(x) и, следовательно, ни один из них не может быть равен f(x). Многочлены h(x), удовлетворяющие условию теоремы 20 и указанному ограничению на степень, называются f-разлагающими.

Итак, пусть $f(x) = x^n + a_{n-1}x^{n-1} + ...+ a_1x + a_0$ многочлен из $F_q[x]$, не имеющий кратных множителей. На основании теоремы 20 задача факторизации f(x) сводится к нахождению f-разлагающих многочленов, являющиеся решениями сравнения $h^q(x) \equiv h(x) \pmod{f(x)}$ Для нахождения всех решений этого сравнения воспользуемся китайской теоремой об остатках. Действительно, пусть $f = f_1f_2...f_s$ – искомое разложение f. Тогда, согласно китайской теореме об остатках, для любого набора многочленов $(r_{1(}x), r_2(x),..., r_s(x))$ найдется единственный класс вычетов по модулю f(x) или, что равносильно, единственный многочлен r(x) степени меньшей n такой, что $r(x) \equiv r_i(x) \pmod{f(x)}$ для всех $i\in\{1, 2,..., s\}$. В частности, подходящий многочлен h(x) найдется для произвольного набора $(c_1, c_2,..., c_{s)}$ констант из поля F_q. Для любого $i\in\{1, 2, ..., s\}$ имеет место сравнение $h(x)^q \equiv c_i^q = c_i \equiv h(x) \pmod{f_i(x)}$. В силу взаимной простоты полиномов $f_1, f_2,..., f_s$, имеем $h(x)^q \equiv h(x) \pmod{f(x)}$. Таким образом, для каждого набора из s констант существует соответствующее решение сравнения (2).

Обратно, пусть многочлен h(x) степени меньшей n является решением сравнения (2). На основании леммы 19 имеем $h(x)^q - h(x) = \prod_{c\in F_q}(h(x)-c)$. Сомножители в правой части этого равенства попарно взаимно просты, поэтому каждый из неприводимых многочленов f_i должен делить полином $h(x) - c$ только для одного значения c. Обозначим это значение через c_i. Тогда $h(x) \equiv c_i \pmod{f_i(x)}$. Такие сравнения справедливы для всех $i\in\{1, 2,..., s\}$. Значит, каждому решению сравнения (2) соответствует свой набор $(c_1, c_2,..., c_s)$. Таким образом, между всеми упорядоченными наборами из s констант из поля F_q и всеми многочленами степени меньшей n, удовлетворяющими сравнению (2) существует биекция. Следовательно, сравнение (2) имеет ровно q^s решений.

Для нахождения решений сравнения (2) воспользуемся методом неопределенных коэффициентов. Пусть $h(x) = b_0 + b_1x +... + b_{n-1}x^{n-1}$ (такая запись не означает, что h(x) имеет степень n-1, поскольку b_{n-1},

как и другие коэффициенты h(x) может оказаться равным 0). Если h(x) удовлетворяет сравнению (2), то:

$$b_0 + b_1x^q + ... + b_{n-1}x^{q(n-1)} \equiv b_0 + b_1x + ... + b_{n-1}x^{n-1} \pmod{f(x)} \quad (4)$$

Для всех $i \in \{0,1,.., n-1\}$ поделим x^{qi} с остатком на f(x): $x^{qi} \equiv \sum_{j=0}^{n-1} d_{ij}x^j \pmod{f(x)}$. Подставив эти выражения в (4) и приведя подобные, получим систему линейных однородных уравнений над полем F_q относительно неизвестных b_i:

$$\begin{pmatrix} 0 & d_{1\,0} & \dots & d_{n-1\,0} \\ 0 & d_{1\,1}-1 & \dots & d_{n-1\,1} \\ \dots & \dots & \dots & \dots \\ 0 & d_{1\,n-1} & \dots & d_{n-1\,n-1}-1 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad (5)$$

Внедиагональные элементы столбцов матрицы (обозначим ее через D и назовем матрицей Берлекэмпа) коэффициентов системы (5) представляют собой соответствующие коэффициенты многочленов $x^{qi} \pmod{f(x)}$, записанных по возрастанию степени. Диагональные элементы получены из соответствующих коэффициентов $x^{qi} \pmod{f(x)}$ вычитанием единицы. Заметим, что первый столбец матрицы D всегда нулевой. Следовательно, ранг D меньше n и система (5) имеет ненулевые решения. В частности, всякая константа из F_q является решением (5). Однако константа (как мы уже отмечали сразу после доказательства теоремы 20) не приводит к содержательному разложению многочлена f.

Может оказаться, что ранг r матрицы D равен n-1. Это означает, что многочлен f неприводим над F_q и в этом случае наша задача решена. Если же r<n-1, то существуют f-разлагающие многочлена. Для их нахождения с помощью элементарных преобразований над строками приведем матрицу D к ступенчатому виду. Поскольку сравнение (2) имеет q^s решений, то размерность пространства решений системы (5) равна s (разумеется, s = n – r) и s неизвестных будут свободными. Последовательно придавая свободным неизвестным значения (1, 0,..., 0), (0, 1,..., 0), (0, 0,..., 1) построим фундаментальную систему решений, образующую базис пространства решений системы(5). Обозначим, через $h_1(x)$, $h_2(x)$, ..., $h_s(x)$ многочлены, соответствующие базисным векторам. Поскольку первый столбец матрицы D – нулевой, ясно, что первым свободным неизвестным будет b_0, а соответствующий базисный многочлен $h_1(x) = 1$ не является f-разлагающим. Остальные базисные многочлены $h_2(x),..., h_s(x)$ (если они есть) будут f-разлагающими. Покажем, что, подставляя эти многочлены в соотношение (3) мы получим полное разложение полинома f.

Рассмотрим неприводимые сомножители, скажем, f_1 и f_2 полинома f. При каждом i, принадлежащем множеству {1, 2,...s} найдутся c_{1i} и c_{2i} из F_q такие, что $f_1(x) \mid h_i(x) - c_{1i}$ и $f_2(x) \mid h_i(x) - c_{2i}$. Очевидно, что $c_{11} = c_{21} = 1$. Допустим, что $\forall i \in \{2,...,s\}(c_{1i} = c_{2i})$. Обозначим равные элементы c_{1i} и c_{2i} через c_i. Пусть теперь h(x) – произвольное решение сравнения (2). Поскольку полиномы $h_1, h_2, ..., h_s$ образуют базис пространства решений, $h(x) = \sum_{i=1}^{s} e_i h_i(x)$ при некоторых $e_i \in F_q$. Полином f_1 делит $\sum_{i=1}^{s} e_i (h_i(x) - c_i) = h(x) - \sum_{i=1}^{s} e_i c_i$ Аналогично f_2 делит $h(x) - \sum_{i=1}^{s} e_i c_i$ Таким образом, для каждого решения сравнения (2) подходящие константы в разложении (3) одинаковы для f_1 и f_2. Но ранее на основании китайской теоремы об остатках мы доказали, что для каждого набора констант ($c_1, c_2,..., c_s$) найдется решение сравнения (2). В том числе, должно существовать решение и для набора, в котором $c_1 \neq c_2$. Полученное противоречие доказывает, что любые два множителя многочлена f "отделимы" с помощью хотя бы одного из базисных многочленов $h_2(x),..., h_s(x)$.

Подведем итоги предыдущих рассуждений, сформулировав основные шаги алгоритма разложения многочлена f, не имеющего кратных множителей, над конечным полем F_q:

Алгоритм 21 (Берлекэмпа)

1. Находим для f берлекэмпову матрицу D.
2. Решая над F_q однородную систему линейных уравнений, задаваемую матрицей D, находим количество неприводимых сомножителей в разложении f и базисные f-разлагающие многочлены $h_2,..., h_s$ (если они есть).
3. Находим наибольшие общие делители многочлена f (и уже найденных делителей f) и многочленов h_i–c, пока не получим полного разложения f. (Этот шаг выполняется в случае, когда f – приводим.)

Рассмотрим несколько примеров разложения многочленов над конечными полями с помощью описанных выше методов.

Пример 22

Найдем каноническое разложение многочлена $g(x) = x^6 + 3x^5 + 3x^4 + x^3 + 1$ над полем Z_5. Поскольку (g, g') = 1, то многочлен g не содержит кратных множителей. Имеем:

$x^0 \equiv 1 \pmod g$;

$x^5 \equiv x^5 \pmod g$;

$x^{10} \equiv 4x^2 + 3x^3 + 4x^4 + 4x^5 \pmod g$;

$x^{15} \equiv 4 + x + 2x^3 + 4x^4 \pmod g$;
$x^{20} \equiv 2 + 2x + 3x^3 + 3 + x^4 + x^5 \pmod g$;
$x^{25} \equiv x \pmod g$.

Отметим, что при нахождении остатка от деления, например, x^{20} на g(x) гораздо рациональнее делить с остатком на f полином $4x^9 + 2x^8 + x^6 + 4x^5$, используя уже найденное выражение для $x^{15} \pmod g$, чем выполнять вычисления непосредственно для полинома 20-й степени.

Заметим также, что на основании сравнения $x^{25} \equiv x \pmod g$ можно сделать вывод о том, что полином g(x) разлагается на множители, степень которых не превышает 2. В самом деле, из этого сравнения следует, что g(x) является делителем многочлена $x^{25} - x$. А он, как нам известно, является произведением всех многочленов первой и второй степеней, неприводимых над Z_5.

Записывая найденные остатки в столбцы и вычитая по единице из элементов главной диагонали, составим матрицу D:

$$D = \begin{pmatrix} 0 & 0 & 0 & 4 & 2 & 0 \\ 0 & 4 & 0 & 1 & 2 & 1 \\ 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 3 & 1 & 3 & 0 \\ 0 & 0 & 4 & 4 & 2 & 0 \\ 0 & 1 & 4 & 0 & 1 & 4 \end{pmatrix}$$

С помощью элементарных преобразований, выполняемых только над строками (чтобы не только найти ранг, но и решить соответствующую систему однородных уравнений), приведем матрицу D к виду:

$$D = \begin{pmatrix} 0 & 1 & 0 & 4 & 3 & 4 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Поскольку ранг D равен 3, то s = 6 –3 =3 и, значит, многочлен g(x) раскладывается в произведение трех различных неприводимых сомножителей. Базисные g-разлагающие многочлены: $h_2(x) = x^4 + 2x^3 + 4x$ и $h_3(x) = x^5 + x$.

Следующий (и последний) шаг алгоритма – нахождение наибольших общих делителей полинома f(x) и многочленов $h_i(x)$ – c, где $i \in \{2,3\}$, а c – пробегает элементы поля Z_5. Имеем:
$(g(x), h_3(x)) = x^2 + 2$;
$(g(x), h_3(x) - 1) = x^2 + 2x + 3$;
$(g(x), h_3(x) - 2) = x^2 + x + 1$.

Мы видим, что, используя лишь один g-разлагающий многочлен, мы уже получили три различных делителя полинома g(x). Поэтому вычислять $(g(x), h_2(x) – c)$ нет необходимости и искомое разложение имеет вид $g(x) = (x^2 + 2)(x^2 + 2x + 3)(x^2 + x + 1)$.

Так бывает довольно часто. Но, как показывает следующий пример, далеко не всегда.

Пример 23

Разложим полином $g(x) = x^7 + x^6 + 2x^4 + x^3 + x^2 + 2$ над полем Z_3.

Убедившись, что g(x) взаимно прост со своей производной и следовательно не имеет кратных множителей, построим для него матрицу D:

$$D = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 2 \\ 0 & 2 & 0 & 2 & 1 & 1 & 1 \\ 0 & 0 & 2 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 2 \end{pmatrix}$$

Ранг D равен 4. А базисными g-разлагающими многочленами будут $h_2(x) = x^5 + x$ и $h_3(x) = x^6 + x^4 + x^3 + x^2 + x$. Имеем:
$(g(x), h_2(x)) = x^4 + 1$;
$(g(x), h_2(x) - 1) = x^3 + x^2 + 2$;
$(g(x), h_2(x) - 2) = 1$.

Поскольку $s = 7 – 4 = 3$, то мы не получили пока полного разложения. Поэтому используем второй g-разлагающий многочлен:
$(x^4 + 1, h_3(x)) = x^2 + 2x + 2$;
$(x^4 + 1, h_3(x)-1) = x^2 + x + 2$.

Окончательно получим: $g(x) = (x^3 + x^2 + 2)(x^2 + 2x + 2)(x^2 + x + 2)$.

Отметим, что, если бы мы начали с нахождения полиномов $((g(x), h_3(x) - c)$, мы все равно не обошлись бы без использования другого g-разлагающего многочлена (хотя иногда такая перестановка позволяет сократить количество используемых g-многочленов и, тем самым, ускорить вычисления).

В предыдущих примерах нам попадались многочлены, не имеющие кратных множителей. Рассмотрим теперь случай, когда они есть.

Пример 24

Пусть $g(x) = x^{13} + x^{12} + x^{11} + x^9 + x^8 + 2x^7 + 2x^5 + 2x^4 + x^3 + 2x + 2$ – многочлен над полем Z_3. В силу того, что $(g, g') = x^8 + 2x_7 + x_5 + 2x^4 + 2x^3 + 2x^2 + 2$, то $g(x)$ имеет кратные множители. Многочлен $f = g/(g, g') = x^5 + 2x^4 + x^3 + 2x^2 + 2$ разлагается в произведение первых степеней тех неприводимых сомножителей многочлена g, которые входят в разложение g с показателями степени, не кратными 3. Построив для многочлена f матрицу D и найдя с ее помощью базисные f-разлагающие многочлены, мы придем к следующему разложению:

$$f(x) = (x^3 + 2x + 1)(x^2 + 2x + 2)$$

Возвращаясь к разложению многочлена $g(x)$, выясним, что (g, g') делится на $x^2 + 2x + 2$ в первой степени и не делится на $x^3 + 2x + 1$. Следовательно, множитель $x^2 + 2x + 2$ входит в разложение $g(x)$ во второй степени, а $x^3 + 2x + 1$ – в первой. Нам остается разложить полином $(g, g')/(x^2 + 2x + 2) = x^6 + x^3 + 2$, имеющий нулевую производную. Очевидно, что этот полином является 3-й степенью полинома $x^2 + x + 2$. Окончательно получаем:

$$g(x) = (x^2 + 2x + 2)^3(x^2 + 2x + 2)^2(x^3 + 2x + 1).$$

Оценим трудоемкость различных этапов описанного выше метода факторизации многочлена над конечным полем. Поскольку на практике чаще всего приходится разлагать многочлены над простыми конечными полями Z_p, ограничимся рассмотрением только этого случая. (Если разложение ведется над расширением F_q поля Z_p, то временная и емкостная сложность алгоритма естественно возрастут за счет организации вычислений в поле F_q.)

Этап проверки факторизуемого многочлена g степени n на наличие кратных множителей и нахождения многочлена $f = g/(g,g')$, не имеющего таковых, проводится за время $O(n^2)$

Построение матрицы Берлекэмпа имеет временную сложность $O(pn^2)$, а нахождение ее ранга и базиса пространства решений (f-разлагающих многочленов) выполняется за время $O(n^3)$. (Здесь и далее мы обозначаем через n степень многочлена f уже освобожденного от кратных множителей.)

Чтобы оценить временную сложность последнего этапа алгоритма, заметим, что степени f-разлагающих многочленов h_i и их количество ограничены сверху числом n-1. Поэтому на нахождение одного наибольшего общего делителя многочленов f и h_i-с потребуется

время, не превосходящее $O(n^2)$. А с учетов варьирования свободных членов и самих f-разлагающих многочленов получим оценку $O(pn^3)$.

Наши рассуждения показывают, что самым трудоемким оказывается последний этап алгоритма. Однако на практике так бывает далеко не всегда. При p существенно меньших n самым затратным часто оказывается этап, связанный с нахождением f-разлагающих многочленов, а последний этап сопоставим по временным затратам с этапом построения матрицы D. При сопоставимых p и n последние два этапа алгоритма оказываются в среднем примерно равны по трудоемкости. И только, когда p существенно превосходит n, последний этап, а вместе с ним и весь алгоритм требуют больших временных затрат.

Такие отклонения (в приятную для нас сторону) истинного времени исполнения последнего этапа алгоритма от оценочного вызваны следующими обстоятельствами:

1. Число сомножителей s в разложении f лишь ограничено сверху числом n, но в среднем значительно меньше него. В случае, когда f неприводим, s = 1 и последний этап алгоритма и вовсе не выполняется. Очевидно, что s может принимать значения сопоставимые с n лишь в том случае, когда f имеет много множителей малых степеней. Но такие множители легко отделить и не прибегая к алгоритму Берлекэмпа. Например, линейные множители отделяются за время O(pn) с помощью схемы Горнера.
2. Степени f-разлагающих многочленов соответствуют номерам свободных переменных однородной системы линейных уравнений с матрицей D. Чем больше свободных неизвестных (а следовательно и сомножителей в разложении f), тем меньше средняя степень f-разлагающих многочленов. Кроме того, степень самого факторизуемого многочлена также уменьшается с отделением уже найденных неприводимых сомножителей. Правда, для того, чтобы исключить найденные сомножители из дальнейшего рассмотрения, надо убедиться в их неприводимости, но для сомножителей малых степеней это делается очень просто.
3. Достаточно часто для полного разложения нет необходимости использовать все f-разлагающие многочлены (такая ситуация встретилась нам в примере 22). К сожалению, в общем случае нельзя заранее усмотреть, какой из f-разлагающих многочленов окажется “полезнее”.

Таким образом, описанный выше алгоритм факторизации полиномов над конечными полями является весьма эффективным. Но

лишь до тех пор, пока количество элементов поля, над которым ведется разложение, относительно невелико. Если же мощность поля велика, то последний этап рассмотренного алгоритма имеет неприемлемую временную сложность и нуждается в совершенствовании.

С этого момента мы возвращаемся к рассмотрению общего случая и полагаем, что многочлен факторизуется над полем F_q.

Итак, пусть мы уже нашли f-разлагающий многочлен h. Тогда некоторые из многочленов h - c, где c пробегает элементы поля F_q, должны иметь нетривиальные общие делители с f. С другой стороны, в силу попарной взаимной простоты полиномов h – c, нетривиальные НОД с f могут иметь не более чем s из них. (Через s мы, как и прежде, обозначаем количество неприводимых множителей в разложении f.)

Учитывая, что два полинома имеют общие корни тогда и только тогда, когда их результант равен 0, и рассматривая результант F(y) = R(f, h – y) как полином от y, приходим к выводу, что его корнями являются те и только те константы c поля F_q, для которых многочлены f и h - c имеют нетривиальное разложение.

Для нахождения коэффициентов F(y) можно напрямую вычислить определитель R(f, h – y). Альтернативный метод – выбрать n+1 различных элементов c_i из F_q, для каждого из них посчитать результанты R(f, h – c_i) и, имея значения r_i полинома F(y) в n+1 точках, воспользоваться интерполяционной формулой Лагранжа: $F(y) = \sum_{i=0}^{n} r_i \prod_{j \neq i} \frac{y - y_j}{y_i - y_j}$. Такой способ хорош еще и тем, что некоторые r_i могут оказаться равными нулю и мы сразу получим искомые корни F(y). Впрочем, при значениях q многократно превышающих n вероятность такого успеха невелика. Но в людом случае мы получим многочлен степени, не превышающей n, знание корней которого приблизит нас к разложению f.

Таким образом, задача факторизации многочлена над большим конечным полем свелась к своему частному случаю: отделению линейных множителей.

Поскольку последняя проблема имеет и самостоятельное значение, мы рассмотрим ее отдельно. Итак, пусть F(x) – многочлен над конечным полем F_q и нам нужно найти его корни, лежащие в F_q. Прежде всего, заметим, что общий случай можно свести к ситуации, когда интересующий нас многочлен разлагается над F_q в произведение попарно различных линейных множителей. В самом деле, нами доказано, что все q корней многочлена $x^q – x$ различны и множество есть в точности множество элементов F_q. Поэтому многочлен f(x) =

$(F(x), x^q - x)$ есть произведение первых степеней линейных сомножителей $F(x)$.

Методы отыскания корней $f(x)$ в значительной мере определяются параметрами поля F_q. При малых q вполне эффективны схема Горнера и прямой перебор элементов поля F_q. Случай большого q обычно подразделяют на три подслучая: q – большое простое число; q – степень небольшого простого числа p; q – степень большого простого числа. Мы ограничимся рассмотрением лишь первого случая. (С методами отыскания корней полиномов над большими конечными полями, не являющимися простыми, можно ознакомиться, например, в [1].)

Пусть $f(x) = \prod_{i=1}^{n}(x - c_i)$ и $b \in Z_p$. Тогда $f(x-b) = \prod_{i=1}^{n}(x - (b + c_i))$

Таким образом, $f(x - b)$ также является произведением n попарно различных линейных множителей. Следовательно, $f(x - b)$ делит полином $x^p - x$. Но $x^p - x$ разлагается в произведение трех сомножителей x, $(x^{(p-1)/2} - 1)$ и $(x^{(p-1)/2} + 1)$ (напомним, что p – большое простое число и, значит, p – нечетно). Если свободный член $f(x - b)$ равен 0, то $f(b) = 0$, и мы уже нашли один из корней $f(x)$.Поэтому, не нарушая общности рассуждений, можно считать, x не делит $f(x - b)$ и

$$f(x - b) = (f(x - b), x^{(p-1)/2} - 1)(f(x - b), x^{(p-1)/2} + 1).$$

Если b таково, что $x^{(p-1)/2}$ не сравнимо ни с 1, ни с –1 по модулю $f(x-b)$, то приведенное выше равенство дает нам нетривиальное разложение $f(x-b)$, а значит и $f(x)$ на два множителя. Продолжая этот процесс, мы рано или поздно отыщем корень $f(x)$.

Если же $f(x-b)$ совпадет с одним из сомножителей в правой части последнего равенства, то можно взять другое b. Учитывая, что сравнение $x^{(p-1)/2} \equiv \pm 1 (\mathrm{mod}\, f(x - b))$ выполняется довольно редко, мы получим достаточно эффективный способ нахождения корней многочлена над простым конечным полем Z_p. Поскольку при больших p степень $(p-1)/2$ велика процесс нахождения НОД полиномов $f(x-b)$ и $x^{(p-1)/2} - 1$ следует начинать лишь убедившись, что он приведет к нетривиальному разложению $f(x-b)$. К счастью, проверить, что для данного b это так (или не так) можно весьма быстро, если возведение x в степень $p(p-1)/2$ по модулю $f(x-b)$ проводить с помощью уже упоминавшегося бинарного алгоритма. Отметим, что такая проверка одновременно является решающим шагом в нахождении интересующих нас НОД.

Рассмотрим пример, который позволит нам проиллюстрировать одновременно и факторизацию многочлена над простым полем, ха-

рактеристика которого – большое простое число, и описанный выше способ отыскания корней.

Пример 25

Разложим многочлен $f(x) = x^6 + 5x^2 + 62x + 8$ на неприводимые сомножители над полем Z_{73}. Имеем:

$$x^{73} \equiv 44x^5 + 48x^4 + 41x^3 + 8x^2 + 47x \,(\mathrm{mod} f(x))$$

$$x^{73} \cdot (44x^5 + 48x^4 + 41x^3 + 8x^2 + 47x) \equiv$$

$$\equiv 15x^5 + 5x^4 + 32x^3 + 39x^2 + 10x + 13 \,(\mathrm{mod} f(x))$$

$$x^{73} \cdot (15x^5 + 5x^4 + 32x^3 + 39x^2 + 10x + 13) \equiv$$

$$\equiv 8x^5 + 26x^4 + 36x^3 + 47x^2 + 33x + 62 \,(\mathrm{mod} f(x))$$

$$x^{73} \cdot (8x^5 + 26x^4 + 36x^3 + 47x^2 + 43x + 62) \equiv$$

$$\equiv 39x^5 + 63x^4 + x^3 + 36x^2 + 2x + 56 \,(\mathrm{mod} f(x))$$

$$x^{73} \cdot (39x^5 + 63x^4 + x^3 + 36x^2 + 2x + 56) \equiv$$

$$\equiv 33x^5 + 44x^4 + 7x^3 + 39x^2 + 3x + 48 \,(\mathrm{mod} f(x))$$

Таким образом, матрица Берлекэмпа для многочлена f(x) имеет вид:

$$D = \begin{bmatrix} 0 & 0 & 13 & 62 & 56 & 48 \\ 0 & 46 & 10 & 33 & 2 & 3 \\ 0 & 8 & 38 & 47 & 36 & 39 \\ 0 & 41 & 32 & 35 & 1 & 7 \\ 0 & 48 & 5 & 26 & 62 & 44 \\ 0 & 44 & 15 & 8 & 39 & 32 \end{bmatrix}$$

Возьмем один из f-разлагающих многочленов – $h(x) = x^4 + 19x^3 + 23x^2 + 21x$. Составим результант полиномов f(x) и h(x)-y.

$$R(f, h - y) = \begin{vmatrix} 1 & 0 & 0 & 0 & 5 & 62 & 8 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 5 & 62 & 8 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 5 & 62 & 8 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 5 & 62 & 8 \\ 1 & 19 & 23 & 21 & -y & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 19 & 23 & 21 & -y & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 19 & 23 & 21 & -y & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 19 & 23 & 21 & -y & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 19 & 23 & 21 & -y & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 19 & 23 & 21 & -y \end{vmatrix}$$

Вычислив этот определитель, получим многочлен от переменной y. Знание корней этого многочлена, лежащих в $\mathbf{Z}_{73}$, приведет нас к разложению исходного многочлена f(x). $R(y) = y^6 + 20y^5 + 42y^4 + 30y^3 + 6y^2 + 49y + 23$. Учитывая, что однократными корнями многочлена $y^{73} - y$ над полем $\mathbf{Z}_{73}$ являются все элементы поля, мы можем ограничиться рассмотрением, многочлена $R_1(y) = (R(y), y^{73} - y) = y^3 + 10y^2 + 44y + 13$.

Возьмем и = 0. Найдем $y^{36} (\mathrm{mod}\ R_1(y))$, используя бинарный алгоритм.

$y^4 \equiv 56y^2 + 62y + 57 \ (\mathrm{mod}\ R_1(y))$;

$y^8 \equiv (56y^2 + 62y + 57)^2 \equiv 42y^2 + 62y + 41 \ (\mathrm{mod}\ R_1(y))$;

$y^{16} \equiv (42y^2 + 62y + 41)^2 \equiv 45y^2 + 56y + 69 \ (\mathrm{mod}\ R_1(y))$;

$y^{32} \equiv (45y^2 + 56y + 69)^2 \equiv 3y^2 + 67y + 62 \ (\mathrm{mod}\ R_1(y))$;

$y^{36} \equiv (3y^2 + 67y + 62)(56y^2 + 62y + 57) \equiv 17y^2 + 5y + 22 \ (\mathrm{mod}\ R_1(y))$;

Таким образом, $y^{36} - 1 \equiv 17y^2 + 5y + 21 \ (\mathrm{mod}\ R_1(y))$ и мы приходим к нетривиальному разложению $R_1(y) = (17y^2 + 5y + 21)(43y+18) = (y^2 + 69y + 27)(y+14)$.

Действуя аналогично, мы получим разложение $R_1(y)$ на линейные множители: $R_1(y) = (y + 57)(y + 12)(y + 14)$.

Вернемся к разложению f(x). Теперь мы знаем, какими должны быть свободные члены полинома h(x) для того, чтобы его НОД с f(x) был нетривиален. $(f(x), h(x) + 14) = x^2 + 22x + 22$;

$(f(x), h(x) + 12) = x^2 + 30x + 37$;

$(f(x), h(x) + 57) = x^2 + 21x + 14$.

Окончательно получаем:

$$f(x) = (x^2 + 22x + 22)(x^2 + 30x + 37(x^2 + 21x + 14).$$

С некоторыми другими методами факторизации полиномов над конечными полями можно ознакомиться в [1] и [4].

Литература

1. Лидл Р., Нидеррайтер Г. Конечные поля. Т.1. – М.: Мир, 1988.
2. Лидл Р., Нидеррайтер Г. Конечные поля. Т.2. – М.: Мир, 1988.
3. Кнут Д. Искусство программирования для ЭВМ. Т.2. Получисленные алгоритмы. – М.: Мир, 1977.
4. Панкратьев Е.В. Компьютерная алгебра. Факторизация многочленов. – М.: МГУ, 1988.
5. Айерленд К., Роузен М. Классическое введение в современную теорию чисел. – М.: Мир, 1987.
6. Калужнин Л.А. Введение в общую алгебру. – М.: Наука, 1973.
7. Ноден П., Китте К. Алгебраическая алгоритмика. – М.: Мир, 1999.
8. Дэвенпорт Дж., Сирэ И., Турнье Э. Компьютерная алгебра. – М.: Мир, 1991.
9. Ван дер Варден Б.Л. Алгебра. – М.: Наука, 1976.
10. Ленг С. Алгебра. – М.: Мир, 1968.
11. Бурбаки Н. Алгебра. Многочлены и поля. Упорядоченные группы. –. М.: Мир, 1965.

Содержание