УДК 512.4

РАЗЛОЖЕНИЕ МНОГОЧЛЕНОВ НАД КОНЕЧНЫМ ПОЛЕМ НА НЕПРИВОДИМЫЕ СОМНОЖИТЕЛИ

А.В. Спиваковский, В.А. Крекнин

(Херсонский государственный педагогический университет, Украина)

Для реализации такого разложения существует достаточно простой и эффективный метод, который назван по имени его автора алгоритмом Берлекемпа (1). В книге (1) рассматривается также другой алгоритм разложения многочленов на неприводимые сомножители для случая конечного поля. В настоящей статье предлагается модификация второго способа решения этой задачи, которая в отдельных частных случаях может быстрее привести к цели, чем рассматриваемые в книге (1) алгоритмы. Для обоснования этой модификации нам будут необходимы некоторые факты из теории конечных полей.

Пусть F – конечное поле, состоящее из q элементов, $q = p^m$, где p – простое число. Если L – конечное расширение поля F степени s, то поле L содержит $r = q^s$ элементов. Для произвольного элемента b поля L положим $\varphi(b) = b^q$. Известно, что отображение φ является автоморфизмом поля L. Пусть $f(x) = x^s + a_1x^{s-1} + a_2x^{s-2} + \ldots + a_{s-1}x + a_s$ – неприводимый многочлен степени s над полем F. Если α - один из корней многочлена f(x), то множество всех корней многочлена f(x) исчерпывается элементами $\alpha, \varphi(\alpha), \varphi^2(\alpha), \ldots, \varphi^{s-1}(\alpha)$. Предположим, что $g(x) = f(x)*h(x)$, где h(x) – многочлен над полем F, отличный от константы и взаимно простой с f(x). Пусть $t_1(x)$ - остаток от деления многочлена x^q на g(x), $t_{k+1}(x)$ – остаток от деления многочлена $(t_k(x))^q$ на g(x), k = 1, 2, 3, …,s-1. Обозначим через $w_j(x)$ – элементарный симметрический многочлен степени j от переменных $t_1(x), t_2(x), \ldots, t_s(x)$. Пусть, наконец, $z_j(x)$ – остаток от деления многочлена $w_j(x)$ на g(x). Из равенства $f(\alpha) = 0$ вытекает, что $z_j(\alpha) = a_j$, $j = 1,2, \ldots, s$. Отсюда следует, что f(x) является общим делителем многочленов $z_j(x) - a_j$ и g(x). В самом деле, если $z_j(x) - a_j = f(x)*d(x) + r(x)$, то при $x = \alpha$ получим, что $r(\alpha) = 0$. Так как α - корень неприводимого над полем F многочлена f(x), а степень r(x) меньше степени f(x), то r(x) = 0.

Приступим теперь к описанию алгоритма разложения многочлена g(x) степени n, определенного над полем F, на неприводимые множители. Предположим сначала, что многочлен g(x) имеет кратные корни. Пусть u(x) – наибольший общий делитель g(x) и его формальной производной. Тогда в разложение многочлена g(x)/u(x) входят в первой степени все неприводимые сомножители из разложения g(x). Таким образом, с самого начала можно предполагать, что g(x) не содержит кратных множителей.

Построим систему многочленов $h_1(x), h_2(x), \ldots, h_i(x)$ по следующему правилу: $h_1(x)$ – наибольший общий делитель многочленов g(x) и

$t_1(x) – x$; $h_2(x)$ - наибольший общий делитель многочленов $g(x)/h_1(x)$ и

$t_2(x) – x; \ldots h_i(x)$ - наибольший общий делитель многочленов

$g(x)/(h_1(x)* h_2(x)*\ldots* h_{i-1}(x))$ и $t_i(x) – x$. Процесс построения многочленов $h_j(x)$ заканчивается самое большее на шаге с номером v, равным целой части числа n/2. Если $h_v(x) \neq 1$, то $h_v(x)$ - неприводимый над полем F многочлен. Из способа получения многочленов $h_i(x)$ вытекает, что $h_i(x)$ либо равен 1, либо является произведением неприводимых многочленов степени i. В частности, если многочлен $h_i(x)$ имеет степень i, то он неприводим. В случае, когда степень $h_i(x)$ больше i, то для отыскания неприводимых сомножителей, входящих в разложение этого многочлена, будем искать наибольшие общие делители многочлена $h_i(x)$ с многочленами $z_j(x) –a$, $j = 1,2,\ldots,i$, a – произвольный элемент поля F. Если $z_j(x) – a$ делится на $h_i(x)$, то остаток от деления $z_j(x) – b$ на $h_i(x)$

равен константе. Этот факт обнаруживается при первой же попытке, и при его наличии поиск наибольших общих делителей $h_i(x)$ и $z_j(x) – a$ при заданном значении j можно сразу прекратить. Если же $z_j(x) –a$ не делится на $h_i(x)$ ни при каком значении $a \in F$, то $h_i(x)$ разлагается в произведение нескольких многочленов, которые являются наибольшими общими делителями многочлена $h_i(x)$ и $z_j(x) – b$, когда b принимает всевозможные значения из поля F. Если при это степень какого- либо сомножителя равна I, то указанный сомножитель является неприводимым многочленом над полем F. Дальнейшей проверке его можно не подвергать и сразу внести в список неприводимых сомножителей из разложения многочлена g(x). Остальные сомножители в разложении $h_i(x)$ следует подвергнуть дальнейшему разложению путем отыскания наибольшего общего делителя этих сомно-жителей и многочленов $z_u(x) – b$, при $u \neq j$, $0 < u < i + 1$, $b \in F$. Таким способом многочлен $h_i(x)$, а вместе с ним и многочлен g(x) будет разложен на неприводимые сомножители. В самом деле, если многочлен

$$x^i – b_1x^{i-1} + b_2x_{i-2} + \ldots +(-1)^{i-1} b_{i-1} x +(-1)^i b_i ,$$

неприводим над полем F и является делителем многочлена g(x), то он является наибольшим общим делителем системы многочленов $\{ z_1(x) – b_1, z_2(x) – b_2, \ldots, z_i(x) – b_i\}$. Описанный способ разложения хорошо реализуется на компьютере, так как его основным элементом является построение наибольшего общего делителя двух многочленов с помощью алгоритма Евклида. Кроме того, многочлены $z_j(x)$ для многочлена $h_{i+1}(x)$ легко можно получить из соответствующих многочленов для $h_i(x)$ с помощью рекуррентной формулы: $z_j(x)$ (для $h_{i+1}(x)$) = $z_j(x)$ (для $h_i(x)$) + $z_{j-1}(x)$ (для $h_i(x)$)*$t_j(x)$.

Предложенный метод быстро приводит к цели, когда многочлены $h_1(x)$, $h_2(x)$,..., $h_i(x)$ либо равны 1, либо имеют степень, равную своему индексу. С худшей стороны этот метод проявляет себя, когда $g(x) = h_i(x)$, причем g(x) является делителем многочленов $z_1(x) – a_1$, $z_2(x) – a_2, \ldots, z_k(x) – a_k$, для некоторых $a_1, a_2, \ldots, a_k \in F$.