Разложение многочлена на неприводимые множители

Рассмотрим самый общий случай. Пусть дано некоторое поле многочленов ***GF***(q), где $q = p^n$, n — степень модуля q, а p — характеристика. Обозначим через $g_1(x)$, $g_2(x)$, ..., $g_{q-1}(x)$ различные неприводимые многочлены над полем чисел $GF(p)$, отвечающие *примитивным* корням: $c_1, c_2, \ldots, c_{q-1}$. Утверждается, что существует единственно возможное разложение многочлена $x^{q-1} - 1$ на множители $g_i(x)$; или, что одно и то же, каждый элемент c_i является корнем многочлена $x^{q-1} - 1$; или, наконец, исходный приводимый многочлен можно представить в виде произведения *порождающего* $g(x)$ и *проверочного* $h(x)$ многочленов:

$$x^{q-1} - 1 = \prod_{i=1}^{q-1} g_i(x) = \prod_{i=1}^{q-1} (x - c_i) = g(x)h(x),$$

$$g(x) = (x - c)(x - c^p)(x - c^{p^2}) \ldots (x - c^{p^k - 1}),$$

$$h(x) = \prod_j (x - c^j).$$

Здесь c — примитивный корень порождающего многочлена $g(x)$, а для проверочного многочлена $h(x)$ берутся те степени c^j, которые не вошли в многочлен $g(x)$. Как видим, действия с многочленами во многом схожи с действиями над числами. Приводимый многочлен вида $x^{q-1} - 1$ играет роль составного числа a, его примитивные корни $c_1, c_2, \ldots, c_{q-1}$ ассоциируются с простыми сомножителями $p_1, p_2, \ldots, p_k$, а последняя формула разложения на множители аналогична каноническому разложению составного числа $a = p_1^{n1} p_2^{n2} \ldots p_k^{nk}$. Многочлены $g(x)$ и $h(x)$ играют роль двух делителей числа $a = g \cdot h$. Корни исходного многочлена играют роль базиса, по которому многочлены $g(x)$ и $h(x)$ могут быть разложены. Таким образом, *теория полей многочленов* смыкается с *теорией линейных пространств*. Покажем, как это осуществляется практически.

Если c — примитивный корень многочлена $g(x)$, то

$$g(c) = g_0 + g_1c + g_2c^2 + \ldots + g_nc^n = 0.$$

Выразим степени корней c^n и c^{n+1} через линейную комбинацию младших степеней корней $c, c^2, \ldots, c^{n-1}$ $(g_n = 1)$:

$$c^n = g_0 + g_1c + g_2c^2 + \ldots + g_{n-1}c^{n-1},$$

$$c^{n+1} = g_0c + g_1c^2 + g_2c^3 + \ldots$$

$$\ldots + g_{n-1}(g_0 + g_1c + g_2c^2 + \ldots + g_{n-1}c^{n-1}).$$

Следовательно, все степени c^i при $i > n$ линейно выражаются через первые n степеней; число таких комбинаций не превышает величину $q - 1$. Следует также иметь в виду, что не только $g(c) = 0$, но и

$$g(c^2) = g(c^3) = \ldots = g(c^{q-1}) = 0.$$

Пример 1. Рассмотрим поле многочленов ***GF***(q) по модулю неприводимого многочлена

$g(x) = x^2 + x + 1$. Пусть примитивным корнем многочлена $g(x)$ является корень c, тогда $g(c) = c^2 + c + 1 = 0$. Так как $q = 2^3 = 8$, то циклический порядок корня c равен $q - 1 = 7$. Все корни степени $i > 2$ выражаются через c и c^2, при этом $g(c)$ берется за модуль:

$$c^3 = (c^3 + c + 1) \cdot 1 + (c + 1) = c + 1,$$

$$c^4 = (c^3 + c + 1) \cdot c + (c^2 + c) = c^2 + c,$$

$$c^5 = (c^3 + c + 1) \cdot c^2 + (c^3 + c^2) = c^2 + c + 1,$$

$$c^7 = (c^3 + c + 1) \cdot c^3 + (c^4 + c^3) = c^2 + 1.$$

Проверим, что числа c, c^2 и c^4 действительно являются корнями многочлена $g(x) = x^2 + x + 1$:

$$g(c) = c^3 + c + 1 = c + 1 + c + 1 = 0,$$

$$g(c^2) = c^6 + c^2 + 1 = c^2 + 1 + c^2 + 1 = 0,$$

$$g(c^4) = c^{12} + c^4 + 1 = c^5 + c^4 + 1 = 0.$$

Отсюда порождающий многочлен $g(x)$ раскладывается на следующие примитивные множители:

$$g(x) = x^2 + x + 1 = (x + c)(x + c^2)(x + c^4),$$

на долю же проверочного многочлена $h(x)$ приходятся все остальные степени корня c:

$$h(x) = (x + c^3)(x + c^5)(x + c^6)(x + c^7).$$

Таким образом, исходный приводимый многочлен $x^7 + 1$ может быть разложен *каноническим* образом в расширенном поле примитивных корней (аналог поля комплексных чисел):

$$x^7 + 1 = (x + c)(x + c^2)(x + c^3)(x + c^4)(x + c^5)(x + c^6)(x + c^7),$$

и *неканоническим*, где в скобках стоят простые сомножители (аналог поля действительных чисел):

$$x^7 + 1 = (x^3 + x + 1)(x^3 + x^2 + 1)(x + 1),$$

а также в виде двух сомножителей:

$$x^7 + 1 = g(x)h(x) = (x^3 + x + 1)(x^4 + x^2 + x + 1).$$

Если в роли модуля будет выступать порождающий многочлен $g(x) = x^3 + x^2 + 1$, то его примитивный корень d даст несколько отличный цикл высших степеней корней, а именно:

$$d^3 = d^2 + 1,\ d^4 = d^2 + d + 1,\ d^5 = d + 1,\ d^6 = d^2 + d,$$

во всем же остальном процедура не изменится.

Пример 2. Составим полную таблицу неприводимых многочленов $g_i(x)$ поля вычетов $\boldsymbol{GF}(2^4)$ по модулю $g(x) = x^4 + x + 1$ над числовым полем $GF(2)$ (табл. 2.82).

Таблица 2.82

c^i	$k \cdot c^3 + l \cdot c^2 + m \cdot c + n$	$g_i(x)$
c^1	c	$x^4 + x + 1$
c^2	c^2	$x^4 + x + 1$
c^3	c^3	$x^4 + x^3 + x^2 + x + 1$
c^4	$c + 1$	$x^4 + x + 1$
c^5	$c^2 + c$	$x^2 + x + 1$
c^6	$c^3 + c^2$	$x^4 + x^3 + x^2 + x + 1$
c^7	$c^3 + c + 1$	$x^4 + x^3 + 1$
c^8	$c^2 + 1$	$x^4 + x + 1$
c^9	$c^3 + c$	$x^4 + x^3 + x^2 + x + 1$
c^{10}	$c^2 + c + 1$	$x^2 + x + 1$
c^{11}	$c^3 + c^2 + c$	$x^4 + x^3 + 1$
c^{12}	$c^3 + c^2 + c + 1$	$x^4 + x^3 + x^2 + x + 1$
c^{13}	$c^3 + c^2 + 1$	$x^4 + x^3 + 1$
c^{14}	$c^3 + 1$	$x^4 + x^3 + 1$
c^{15}	1	$x + 1$

Заполнение таблицы неприводимых многочленов начнем с исходного многочлена. Так как

$$g(x) = (x - c)(x - c^2)(x - c^4)(x - c^8),$$

против степеней c, c^2, c^4 и c^8 можно писать многочлен $g(x)$. Далее, выразим все степени c^i через c, c^2 и c^3, как это было сделано в предыдущем случае. Чтобы найти все остальные неприводимые множители, необходимо поступить следующим образом. Возьмем произвольный корень $a = c^{14} = c^3 + 1$. Тогда

$$ga\ (x) = (x - a)(x - a^2)(x - a^4)(x - a^8).$$

Так как

$$a^2 = c^{28-15} = c^{13} = c^3 + c^2 + 1,$$

$$a^4 = c^{56-45} = c^{11} = c^3 + c^2 + c,$$

$$a^8 = c^{112-105} = c^7 = c^3 + c + 1,$$

можно написать

$$g_a(x) = (x - c^{14})(x - c^{13})(x - c^{11})(x - c^7) =$$

$$= [x^2 - (c^{14} + c^{13})x + c^{12}] \cdot [x - c^{11}] \cdot [x - c^7] =$$

$$= (x^2 - c^2x + c^{12}) \cdot (x - c^{11}) \cdot (x - c^7) =$$

$$= [x^3 - (c^{11} + c^2)x^2 + (c^{12} + c^{13})x - c^8] \cdot (x - c^7) =$$

$$= (x^3 - c^9x^2 + cx - c^8) \cdot (x - c^7) =$$

$$= x^4 - (c^9 + c^7)x^3 + (c + c)x^2 - (c^8 + c^8)x + c^{15}.$$

Следовательно, против корней c^7, c^{11}, c^{13} и c^{14} ставим неприводимый многочлен $g_a(x) = x^4 + x^3 + 1$. Затем берется следующий неизвестный корень и предыдущая процедура повторяется. Так происходит последовательное заполнение всей табл. 2.82. Проверка правильности нахождения состоит в выполнении основного тождества:

$x^{15} + 1 = (x^4 + x^3 + 1)(x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)(x + 1).$

Пример 3. Рассмотрим поле $\boldsymbol{GF}(3^2)$ по модулю $g(x) = x^2 + 1$ над полем $GF(3)$. Здесь многочлен $g(x)$ является неприводимым, но он не является и порождающим или образующим многочленом поля, поскольку степени его корня дают единицу уже при c^4, а не 8:

$$c^2 = (c^2 + 1) \cdot 1 + 2 = 2,$$

$$c^3 = (c^2 + 1) \cdot c + 2c = 2c,$$

$$c^4 = (c^2 + 1) \cdot c^2 + 1 = 1,$$

$$c^5 = c,\ c^6 = 2,\ c^7 = 2c,\ c^8 = 1.$$

Аналогичная ситуация возникает и в числовых полях, например, в поле $GF(7)$ элемент 3 является образующим, так как его степени порождают все элементы поля:

$$3^1 = 3, \quad 3^2 = 2, \quad 3^3 = 6, \quad 3^4 = 4, \quad 3^5 = 5, \quad 3^6 = 1,$$

тогда как элемент 2 уже не будет образующим; в самом деле, его степени не дают элементы 3, 5 и 6:

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 1, \quad 2^4 = 2, \quad 2^5 = 4, \quad 2^6 = 1.$$

Поэтому исходным порождающим элементом нужно выбрать другой неприводимый многочлен, например, $g(x) = x^2 + x + 2$. При составлении полной таблицы неприводимых многочленов (табл. 2.83) для случая поля $GF(3)$ действуем аналогично предыдущему примеру. Представителями классов вычетов по модулю 3 могут быть как числа 0, 1, 2, так и числа –1, 0, 1. Отсюда возникают две формы записи неприводимых многочленов с двумя проверочными соотношениями:

$$x^8 + 2 = (x^2 + x + 2)(x^2 + 2x + 2)(x^2 + 1)(x + 1)(x + 2),$$

$$x^8 - 1 = (x^2 + x^3 - 1)(x^4 - x - 1)(x^2 + 1)(x + 1)(x - 1).$$

Таблица 2.83

c^i	$k \cdot c + l$	$g_i(x)$ {0, 1, 2}	$g_i(x)$ {– 1, 0, 1}
c^1	c	$x^2 + x + 2$	$x^2 + x - 1$
c^2	c^2	$x^2 + 1$	$x^2 + 1$
c^3	c^3	$x^2 + x + 2$	$x^2 + x - 1$
c^4	$c + 1$	$x + 1$	$x + 1$
c^5	$c^2 + c$	$x^2 + 2x + 2$	$x^2 - x - 1$
c^6	$c^3 + c^2$	$x^2 + 1$	$x^2 + 1$
c^7	$c^3 + c + 1$	$x^2 + 2x + 2$	$x^2 - x - 1$
c^8	$c^2 + 1$	$x + 2$	$x - 1$

Полные таблицы неприводимых многочленов и линейные комбинации корней для полей $\boldsymbol{GF}(5^2)$, $\boldsymbol{GF}(3^3)$ и $\boldsymbol{GF}(2^5)$ приведены, соответственно, в табл. 2.84, 2.85 и 2.86.

Таблица 2.84

c^i	$k \cdot c + l$	$g_i(x)$
c^1	c	$3x^2 + 2x + 1$
c^2	$c + 3$	$x^2 + 2x + 4$
c^3	$4c + 3$	$x^2 + 3$
c^4	$2c + 2$	$x^2 + x + 1$
c^5	$4c + 1$	$3x^2 + 2x + 1$
c^6	2	$x^2 + 4x + 4$
c^7	$2c$	$x^2 + 2x + 3$
c^8	$2c + 1$	$x^2 + 4x + 1$
c^9	$3c + 1$	$x^2 + 2$
c^{10}	$4c + 4$	$x^2 + 2x + 4$
c^{11}	$3c + 2$	$x^2 + 2x + 3$
c^{12}	4	$x^2 + 3x + 1$
c^{13}	$4c$	$x^2 + 4x + 2$
c^{14}	$4c + 2$	$x^2 + 3x + 4$
c^{15}	$c + 2$	$x^2 + 3$
c^{16}	$3c + 3$	$x^2 + 4x + 1$
c^{17}	$c + 4$	$x^2 + 4x + 2$
c^{18}	3	$x^2 + x + 4$
c^{19}	$3c$	$x^2 + 3x + 3$
c^{20}	$3c + 4$	$x^2 + x + 1$
c^{21}	$2c + 4$	$x^2 + 2$
c^{22}	$c + 1$	$x^2 + 4$
c^{23}	$2c + 3$	$x^2 + 3x + 3$
c^{24}	1	$x + 1$

Таблица 2.85

c^i	$l \cdot c^2 + m \cdot c + n$	$g_i(x)$
c^1	c	$x^3 + 2x + 1$
c^2	c^2	$x^3 + x^2 + x + 2$
c^3	$c + 2$	$x^3 + 2x + 1$
c^4	$c^2 + 2c$	$x^3 + x^2 + 2$
c^5	$2c^2 + c + 2$	$x^3 + 2x^2 + x + 1$
c^6	$c^2 + c + 1$	$x^3 + x^2 + x + 2$
c^7	$c^2 + 2c + 2$	$x^3 + x^2 + 2x + 1$
c^8	$2c^2 + 2$	$x^3 + 2x^2 + 2x + 2$
c^9	$c + 1$	$x^3 + 2x + 1$
c^{10}	$c^2 + c$	$x^3 + x^2 + 2$
c^{11}	$c^2 + c + 2$	$x^3 + x^2 + 2x + 1$
c^{12}	$c^2 + 2$	$x^3 + x^2 + 2$
c^{13}	2	$x + 1$
c^{14}	$2c$	$x^3 + 2x + 2$
c^{15}	$2c^2$	$x^3 + 2x^2 + x + 1$
c^{16}	$2c + 1$	$x^3 + 2x + 2$
c^{17}	$2c^2 + c$	$x^3 + 2x^2 + 1$
c^{18}	$c^2 + 2c + 1$	$x^3 + x^2 + x + 2$
c^{19}	$2c^2 + 2c + 2$	$x^3 + 2x^2 + x + 1$
c^{20}	$2c^2 + c + 1$	$x^3 + 2x^2 + 2x + 2$
c^{21}	$c^2 + 1$	$x^3 + x^2 + 2x + 1$
c^{22}	$2c + 2$	$x^3 + 2x + 2$
c^{23}	$2c^2 + 2c$	$x^3 + 2x^2 + 1$
c^{24}	$2c^2 + 2c + 1$	$x^3 + 2x^2 + 2x + 2$
c^{25}	$2c^2 + 1$	$x^3 + 2x + 1$
c^{26}	1	$x + 2$

Таблица 2.86

c^i	$j c^4 + k c^3 + l c^2 + m c + n$	$g_i(x)$
c^1	c	$x^5+x^4+x^2+x+1$
c^2	c^2	$x^5+x^4+x^2+x+1$
c^3	c^3	$x^5+x^4+x^3+1$
c^4	c^4	$x^5+x^4+x^2+x+1$
c^5	c^4+c^2+c+1	$x^5+x^3+x^2+x+1$
c^6	c^4+c^3+1	$x^5+x^4+x^3+1$
c^7	c^2+1	x^5+x^2+1
c^8	c^3+c	$x^5+x^4+x^2+x+1$
c^9	c^4+c^2	$x^5+x^3+x^2+x+1$
c^{10}	$c^4+c^3+c^2+c+1$	$x^5+x^3+x^2+x+1$
c^{11}	c^4+c^3+1	$x^5+x^4+x^3+x^2+1$
c^{12}	c^4+c	$x^5+x^4+x^3+1$
c^{13}	c^4+c+1	$x^5+x^4+x^3+x^2+1$
c^{14}	c^4+1	x^5+x^2+1
c^{15}	c^4+c^2+1	$x^5+x^4+x^3+x^2+x+1$
c^{16}	$c^4+c^3+c^2+1$	$x^5+x^4+x^2+x+1$
c^{17}	c^3+c^2+1	$x^5+x^4+x^3+1$
c^{18}	c^4+c^3+c	$x^5+x^3+x^2+x+1$
c^{19}	$c+1$	x^5+x^2+1
c^{20}	c^2+c	$x^5+x^3+x^2+x+1$
c^{21}	c^3+c^2	$x^5+x^4+x^3+x^2+1$
c^{22}	c^4+c^3	$x^5+x^4+x^3+x^2+1$
c^{23}	c^2+c+1	$x^5+x^4+x^3+x^2+x+1$
c^{24}	c^3+c^2+c	$x^5+x^4+x^3+1$
c^{25}	$c^4+c^3+c^2$	x^5+x^2+1
c^{26}	c^3+c^2+c+1	$x^5+x^4+x^3+x^2+1$
c^{27}	$c^4+c^3+c^2+c$	$x^5+x^4+x^3+x^2+x+1$
c^{28}	c^3+c+1	x^5+x^2+1
c^{29}	c^4+c^2+c	$x^5+x^4+x^3+x^2+x+1$
c^{30}	c^4+c^3+c+1	$x^5+x^4+x^3+x^2+x+1$
c^{31}	1	$x+1$

Для практического задания по теме составления полной таблицы неприводимых многочленов преподаватель может менять порождающий многочлен $g(x)$; $g(x)$ стоит в первых строчках приведенных таблиц; в этом случае происходит перегруппировка строк.