АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ. ВЫЧИСЛЕНИЯ В ЧИСЛОВЫХ ГРУППАХ, КОЛЬЦАХ И ПОЛЯХ

1 Группы

Группой называется множество G, на котором определена ассоциативная бинарная операция $\circ$, которое содержит элемент e такой, что для любого элемента $a \in G$ выполняется

$$e \circ a = a \circ e = a,$$

и существует элемент $\bar{a}$ такой, что

$$a \circ \bar{a} = \bar{a} \circ a = e.$$

Указанный элемент e называется *нейтральным элементом*, или *единицей* группы, элемент $\bar{a}$ называется *симметричным* к элементу a. [1] Легко показать, что единица группы единственна и что элемент, симметричный к данному элементу, также определяется однозначно. Как следствие, в группе можно определить унарную операцию *инверсии* [2], которая сопоставляет каждому элементу a, $a \in G$, симметричный к нему элемент $\bar{a}$. Эта операция является биекцией, т.е. взаимно-однозначным отображением. Если операция $\circ$ коммутативна, то группа называется *коммутативной* или *абелевой*. В дальнейшем мы будем использовать только абелевы группы.

В теории групп используется две равноправных и эквивалентных друг другу терминологических системы: аддитивная и мультипликативная. В аддитивной системе групповую операцию называют операцией сложения, а группы в аддитивной записи для краткости будем назвать иногда *аддитивными* . Группы, операцию в которых называют умножением, именуются далее иногда *мультипликативными* группами.

Операцию аддитивной группы принято обозначать знаком $+$, операцию мультипликативной группы обозначают знаком умножения $\times$, или $\cdot$ или её обозначение, по умолчанию, опускают.

[1] Более распространен термин обратный элемент, но его мы далее будем употреблять только для групп мультипликативной записи.

[2] Другой термин — обращение.

Нейтральный элемент аддитивной группы обозначается 0 и называется *нулем.* Результат $\bar{a}$ *аддитивной инверсии*, то есть элемент аддитивной группы, симметричный к элементу a, обозначатся $-a$ и называется *противоположным* к этому элементу. Нейтральный элемент мультипликативной группы обозначается 1 и называется *единицей.* Результат $\bar{a}$ *мультипликативной инверсии* обозначатся a^{-1} и называется *обратным* к этому элементу.

Ассоциативность операции $\circ$ позволяет записывать кратное произведение

$$(\cdots((a \circ a) \circ a) \circ \cdots a) \circ a,$$

опуская скобки:

$$a \circ a \circ a \circ \cdots \circ a.$$

Такая формула называются *k-ой степенью* элемента a группы (k – число вхождений элемента a в формулу). В аддитивных группах k-я степень элемента a обозначается $k * a$, в мультипликативных группах используется обозначение a^k. По определению, $0 * a = 0$ и $a^{(0)} = 1$.

Композиция

$$a + (-b)$$

операций инверсии и сложения аддитивной группы называется операцией *вычитания* элемента b из элемента a, обозначаемой знаком минус. Результат $a - b$ называется *разностью* элементов a и b. Противоположный к элементу a элемент $-a$ получается как разность $0 - a$.

Композиция

$$a \times b^{-1}$$

операций инверсии и умножения мультипликативной группы называется операцией *деления* элемента a на элемент b, обозначаемой косой чертой /. Результат a/b, или $\frac{a}{b}$ называется *частным* от деления элемента a на элемент b. Обратный к элементу a элемент a^{-1} получается как частное $\frac{1}{a}$.

Рассмотренные выше примеры аддитивных и мультипликативных групп представляют бесконечные группы.

Группа, определенная на конечном множестве G, называется *конечной. Тривиальная(единичная)* группа определена на одноэлементном множестве $\{e\}$ и содержит только единицу. Число элементов конечной группы называется *порядком* группы. Порядок тривиальной группы равен 1, простейшая нетривиальная группа имеет порядок 2.

Порядком элемента g группы G называется наименьшее число n такое, что $g^n = e$. Порядок элемента g иногда далее обозначается ord g.

Элемент, порядок которого равен порядку группы, если он существует, называется *образующим* элементом группы.

Группа, имеющая образующий элемент, называется *циклической* .

Часто конечная группа определяется как фактор-множество бесконечной группы по некоторому отношению эквивалентности. [3]

Так, на множестве Z целых чисел относительно натурального числа m можно определить отношение

$$\{(x, y) \setminus x \equiv y \pmod{m}\},$$

где $x \equiv y (\bmod m)$ означает, что число m делит разность $(x - y)$.[4] Это отношение называется *отношением конгруэнтности по модулю* m, а классы эквивалентности по этому отношению – *классами конгруэнтности* (*или классами вычетов*) *по модулю* m.

Фактор-множество $Z/\equiv \bmod m$ по этому отношению сокращенно обозначают Z_m, аналогично, классы конгруэнтности $[a]_{\equiv \bmod m}$ обозначаются просто $[a]_m$.

[3]Отношением эквивалентности называется однородное бинарное отношение $\approx$, обладающее свойствами транзитивности ($(a \approx b)$ и $(b \approx c)$ влекут $a \approx c$)), рефлексивности ($(a = b)$ влечет $(a \approx b)$) и симметричности ($(a \approx b)$ влечет $(b \approx a)$). Множество, на котором задано это отношение, разбивается на *классы эквивалентности* $[a]_\approx$, где a – *представитель* класса. Совокупность классов эквивалентности есть *фактор-множество* множества A по данному отношению $\approx$, обозначается иногда $A \setminus_\approx$.

[4]Согласно алгоритму деления целых чисел с остатком при заданном ненулевом *делителе* d *делимое* a единственным образом представляется формулой $a = qd + r,\ 0 \le r < |d|$. Число q называется *частным* , а число r называется *остатком от деления* a *на* q. Например, если $a = 5$, а $d = -2$, то $a = (-2)(-2) + 1$, то есть $q = -2,\ r = 1$. Если остаток $r = 0$, то говорят, что d *делит* a, что обозначают $d|a$. Остаток обозначают также $r = a \bmod d$ или $\mathrm{rem}(a, d)$ *Наибольшим общим делителем* целых чисел n и m называется наибольшее число d, являющееся делителем как m, так и n. Это число обозначается НОД(n, m) или просто (n, m). НОД(n, m) существует, тогда и только тогда, когда хотя бы одно из чисел n и m не равно 0. Если НОД$(n, m) = 1$, то числа n и m называются *взаимно простыми* .

Легко видеть, что $x \equiv y \pmod m$ тогда и только тогда, когда $x \bmod m = y \bmod m$, где $x \bmod m$ и $y \bmod m$ – остаток от деления числа x или числа y на m.

На фактор - множестве Z_m можно определить арифметические операции. Сумму классов эквивалентности определяют следующим образом:

$$[x]_m + [y]_m = [x + y]_m.$$

Удобно в качестве представителей классов $[x]_m$ использовать наименьшие неотрицательные элементы $x \bmod m$ классов. Тогда операцию сложения можно описать в обозначениях этих представителей:

$$[x]_m + [y]_m = [(x + y) \bmod m]_m.$$

Упражнение 1.1 Убедитесь, что фактор множество Z_m с только что описанной операцией сложения есть аддитивная группа с нейтральным элементом $[0]_m$ и что противоположный к элементу $[a]_m$ группы есть элемент $-[a]_m = [m - a]_m$.

Аналогично вводится операция умножения по модулю m.

$$[x]_m \times [y]_m = [x \times y]_m = [(x \times y) \bmod m]_m.$$

При этом множество ненулевых классов конгруэнтности $[a]_m,\ a \neq 0$, имеющих обратный класс $[a^{-1}]_m$, где $a \times a^{-1} \bmod m = 1$, образует мультипликативную группу, которая обозначается Z_m^*. Мультипликативной единицей является класс $[1]_m$. Класс $[a]_m$ принадлежит Z_m^* тогда и только тогда, когда числа a и m взаимно просты, то есть не имеют общих множителей. Порядок группы Z_m^* обозначается $\varphi(m)$, и так определенная функция называется функцией Эйлера.

Рассмотренные аддитивная и мультипликативная группы, определённые на множествах Z_m и Z_m^* классов конгруэнтности по модулю m, изоморфны аддитивной и мультипликативной группам, заданным на множестве наименьших неотрицательных представителей этих классов, соответственно с операциями сложения и умножения по модулю m. Поэтому часто вместо группы на фактор множестве рассматривают группы на множестве представителей классов, при этом эти множества $Z_m = \{0, 1, \ldots,\ m - 1\}$ и $Z_m^* = \{a/a$ и m взаимно просты$\}$ представителей обозначают так же, как множества классов. Операции в таких группах ниже обозначаются $+_{\bmod m}$ и $\times_{\bmod m}$ или просто $+$ и $\times$.

Подмножество H группы G, замкнутое относительно операций группы, и являющееся группой с этими же операциями, называется *подгруппой* этой группы.

Классы эквивалентности $[a]_{\approx}$ по этому отношению называются *левыми смежными классами группы G по подгруппе H*. Очевидно, что $h_1 \neq h_2 \to ah_1 \neq ah_2$ для любых $h_1, h_2 \in H$. Действительно, если $ah_1 = ah_2$, то умножая обе части равенства слева на a^{-1}, получим $a^{-1}ah_1 = a^{-1}ah_2 \to h_1 = h_2$, что ведет к противоречию. Значит, число элементов в каждом классе равно порядку подгруппы H. Если подгруппа H такова, что число смежных классов конечно, то это число называется *индексом подгруппы H в группе G* (обозначается $G : H$).

Учитывая, что суммарное число элементов в классах равно порядку группы, получаем для конечной группы следующее утверждение.

Теорема 1.1 (Лагранж) . *Порядок и индекс подгруппы H в группе G делят порядок группы.*

Пример 1.1 Возьмем подгруппу $\{[0]_9, [3]_9, [6]_9\}$ аддитивной группы

$$Z_9 = \{[0]_9, [1]_9, [2]_9, [3]_9, [4]_9, [5]_9, [6]_9, [7]_9, [8]_9\}.$$

Левыми смежными классами являются множества

$$\{[0]_9, [3]_9, [6]_9\},$$
$$\{[1]_9, [4]_9, [7]_9\},$$
$$\{[2]_9, [5]_9, [8]_9\}.$$

Индекс $G : H$ равен 3.

Аналогично определяются правые смежные классы.

Упражнение 1.2 Убедитесь, что левые и правые смежные классы абелевой группы совпадают.

Упражнение 1.3 Покажите, что в конечной группе все различные степени $a^1, a^2, \ldots, a^\delta$ любого элемента составляют циклическую подгруппу, порядок которой равен порядку δ этого элемента (если $l > \delta$, то $a^l = a^{c\delta + (l \bmod \delta)} = a^{l \bmod \delta}$.

Отсюда получаем следующие утверждения:

Следствие 1.1 *Порядок любого элемента конечной группы делит порядок группы.*

Следствие 1.2 *Для любого элемента a конечной группы порядка m имеет место равенство $a^m = e$.*

Следствие 1.3 *Если δ – порядок элемента a группы G, а $n \in N$, то $a^n = e$ тогда и только тогда, когда $\delta | n$.*

Следствие 1.4 *Для любого элемента a конечной группы порядка m имеет место равенство $a^{m-1} = a^{-1}$.*

Следствие 1.5 (Теорема Эйлера) . *Для всякого натурального n и всякого натурального a такого, что* НОД$(a, n) = 1$, *справедливо отношение*

$$a^{\varphi(n)} \equiv 1 (\mathrm{mod}\ n).$$

Пример 1.2 Если $n = 6$, то группа $G = (\{1, 5\}, \times_{\mathrm{mod}\ 6}, 1)$, $\varphi(6) = 2$, $1^2 = 1 \mod 6$, $5^2 = 1 \mod 6$.

Следствие 1.6 (Малая теорема Ферма) . *Для всякого простого числа p и целого числа a, не кратного p, имеет место отношение*

$$a^{p-1} \equiv 1 \ (\mathrm{mod}\ p).$$

Возведение элемента конечной группы в большую степень можно упростить путём приведения показателя степени по модулю m порядка группы:

$$g^n = g^{n \bmod m}.$$

В частности, возведение числа g, такого, что $(g, n) = 1$, в большую степень k по модулю n можно упростить путём приведения показателя степени по модулю $m = \varphi(n)$:

$$g^k \bmod n = g^{k \bmod \varphi(n)} \mathrm{mod}\ n.$$

Теорема 1.2 *Для любой группы G при любом натуральном k порядок m элемента a^k определяется равенством*

$$m = \frac{\delta}{(k, \delta)}, \tag{1}$$

где $\delta =$ord a. В частности, ord $a^k = \delta$ *тогда и только тогда, когда $(k, \delta) = 1$.*

Алгоритм 1.1

ВХОД: Элемент a известной мультипликативной группы G;
коэффициенты $(d_0, d_1, \ldots d_{n-1})$ бинарного разложения
показателя степени $d = d_0 2^{(0)} + d_1 2^1 + \cdots + d_{n-1} 2^{n-1}$.
ВЫХОД: Степень $b = a^d$ элемента a.
1. $b \leftarrow 1$.
2. Для i от 1 до n : $b \leftarrow b^2 a^{d_{n-i}}$.
3. Вернуть b.

Рис. 1: Алгоритм возведения в степень в мультипликативной группе.

Упражнение 1.4 Сформулируйте утверждения, аналогичные следствиям 1.2 – 1.6 и Теореме 1.2 применительно к конечной аддитивной группе.

Рассмотрим методы вычисления порядка элемента группы и нахождения образующих элементов групп, а также элементов высокого порядка.

В приведенных ниже алгоритмах используется свойство, что порядок элемента делит порядок группы (следствие 1.1).

Алгоритмы записаны в мультипликативной символике.

Заметим, что возведение в степень элемента группы можно осуществить быстро, если воспользоваться разложением показателя степени в двоичной системе счисления и использовать алгоритм 1.1 на рис. 1 (так называемый бинарный алгоритм).

Лемма 1.1 (1) . *Для вычисления степени m^n, где m – элемент некоторого кольца, а n – натуральное число, достаточно выполнить не более $2\lfloor\log_2 n\rfloor$ операций умножения.*

Если вместо возведения в степень использовать операцию умножения, то получим алгоритм вычисления аддитивного кратного $k * a$ элемента a.

Упражнение 1.5 Обоснуйте этот алгоритм.

Определение порядка элемента группы при известной факторизации порядка n группы. Порядок элемента группы можно определить по алгоритму 1.2 (см. рис. 2).

Алгоритм 1.2

ВХОД: Элемент $a \in G$, *мультипликативной группы* G *порядка* n,
факторизация $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$.
где p_i, $(i = 1, \ldots, k)$ – разные простые числа.

ВЫХОД: порядок t элемента a.

1. $t \leftarrow n$.
2. Для i от 1 до k :
   2.1 $t \leftarrow t/p_i^{e_i}$.
   2.2 $a_1 \leftarrow a^t$.
   2.3 Пока $a_1 \neq 1$: $a_1 \leftarrow a_1^{p_i}$, $t \leftarrow t \cdot p_i$.
3. Вернуть t.

Рис. 2: Алгоритм определения порядка элемента мультипликативной группы группы .

Упражнение 1.6 Обоснуйте этот алгоритм.

Поиск образующего элемента циклической группы. Приведём вероятностный алгоритм 1.3 (рис. 3) поиска образующего элемента циклической группы. Эффективность алгоритма определяется тем, что группа содержит $\varphi(n)$ образующих элементов, и вероятность того, что случайно выбираемый элемент является образующим равна $\varphi(n)/n > \frac{1}{6 \ln \ln n}$. (см. [2]).

Замечание. Трудности проблемы факторизации можно обойти выбором подходящей группы Z_p^*. При этом обеспечивается и присутствие большого множителя в разложении числа $p - 1$. Сначала выбирается достаточно большое простое число q. Затем случайно выбирают относительно малые числа R, пока не будет получено простое число $p = 2Rq + 1$. Поскольку $p - 1 = 2Rq$, факторизация сводится к факторизации числа R. Если выбирать $R = 1$, то факторизацией $p - 1$ является просто $2q$. Поскольку $\varphi(p - 1) = \varphi(2q) = \varphi(2)\varphi(q) = q - 1$, вероятность того, что случайно выбранный элемент $\alpha \in Z_p^*$ является образующим элементом, есть $\frac{q-1}{2q} \approx \frac{1}{2}$. Простое число вида $p = 2q+1$, где q – простое, называется *безопасным* простым числом [3].

Упражнение 1.7 Обоснуйте этот алгоритм. Переформулируйте алгоритмы 1.1, 1.2 и 1.3 применительно к аддитивной группе и составьте унифицированные описания соответствующих алгоритмов для мультипликативной и аддитивной групп.

Алгоритм 1.3

ВХОД: Порядок n, известной циклической мультипликативной циклической группы G,
факторизация $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$,
где $p_i, \ i = 1, \ldots, k$, – разные простые числа.
ВЫХОД: образующий элемент α группы G.

1. Выбрать случайный элемент α группы G.
2. Для i от 1 до k :
   2.1 $b \leftarrow \alpha^{n/p_i}$.
   2.2 Если $b = 1$, то перейти к 1.
3. Вернуть α.

Рис. 3: Вероятностный алгоритм поиска образующего элемента циклической мультипликативной группы.

Указание. Используйте обобщенное обозначение, например, $g(x, t)$ для функций умножения на константу $t \cdot x$ и функции возведения в степень x^t.

Поиск элемента высокого порядка циклической группы. Иногда требуется найти элементы высокого порядка, не являющиеся образующими элементами.

Пусть α – образующий элемент циклической группы G порядка n и d – делитель числа n. Тогда по теореме 1.2 элемент β порядка d можно получить как $\beta = \alpha^{n/d}$. Если q – простой делитель порядка n циклической группы G, элемент β порядка q можно найти без предварительного поиска образующего элемента α группы G. Для этого выбирают случайно $g \in G$ и вычисляют $\beta = g^{n/q}$, повторяя эти действия, пока не будет получено $\beta, \ \beta \neq 1$.

Упражнение 1.8 Сформулируйте аналогичное правило поиска элемента высокого порядка применительно к аддитивной группе.

Применительно к группе, не являющейся циклической, ввиду отсутствия образующих элементов в ней используют элементы максимального порядка.

Приведем алгоритм 1.4 поиска элемента максимального порядка группы $Z_{p \cdot q}^*$. Пусть $n = p \cdot q$, где p и q – различные нечетные простые числа. Тогда

Алгоритм 1.4

ВХОД: два различных нечетных простых числа p и q,
факторизация чисел $p-1$ и $q-1$.
ВЫХОД: элемент α максимального порядка НОК$(p-1, q-1)$
группы $Z_n^*,\ n = p \cdot q$.
1. Применяя алгоритм 1.3 к $G = Z_p^*$ и факторизацию числа $p-1$,
найти образующий элемент a группы G_p^*.
2. Применяя алгоритм 1.3 к $G = Z_q^*$ и факторизацию числа $q-1$,
найти образующий элемент b группы G_q^*.
3.Найти целое $\alpha,\ 1 \leq \alpha \leq n-1$, удовлетворяющее сравнениям
$\alpha \equiv a \pmod{p}$,
$\alpha \equiv b \pmod{q}$.
4. Вернуть α.

Рис. 4: Алгоритм поиска элемента максимального порядка мультипликативной группы.

$Z_{p \cdot q}^*$ – группа порядка $\varphi(n) = (p-1)(q-1)$, не являющаяся циклической (см. рис. refcaption 1.7).

2 Кольца. Поля. Многочлены над полем

Кольцом называется множество R с операциями сложения и умножения такими, что R является абелевой группой относительно сложения и операция умножения ассоциативна и дистрибутивна относительно операции сложения:

$$(a \times b) \times c = a \times (b \times c),$$

$$a \times (b + c) = a \times b + a \times c \text{ и } (b + c) \times a = b \times a + c \times a.$$

Следствием определения кольца является свойство: для любого a

$$a \times 0 = 0 \times a = 0.$$

Примерами колец являются множества Z целых, Q рациональных и R действительных чисел с операциями сложения и умножения.

Кольцо, в котором $a \times b = 0$ влечет $a = 0$ или $b = 0$ называется *областью целостности.* Если в кольце имеется мультипликативная единица 1, то кольцо называется *кольцом с единицей.* Ниже рассматриваются только кольца с единицей.

Элемент a' кольца с единицей такой, что $a \times a' = 1$ называется *обратным к элементу* a. Элемент, обратный к элементу a кольца, обозначается a^{-1}. Каждый элемент кольца имеет не более одного обратного к нему элемента. Элемент, обратный к нулевому элементу кольца, не существует.

Множество элементов кольца, имеющих обратный элемент, составляет мультипликативную группу кольца R, которая обозначается R^*.

Полем называется кольцо F с единицей, множество ненулевых элементов которого с операцией умножения является абелевой группой. Эта группа называется мультипликативной группой поля.

Примерами бесконечных полей являются поля Q рациональных, R действительных и C комплексных чисел.

Подмножество F поля Q, замкнутое относительно обеих операций и являющееся полем, называется *подполем* , что обозначается $F \subseteq Q$.

Поле, не имеющее подполя, не совпадающего с самим полем, называется *простым* полем. Имеется единственное простое бесконечное поле – поле Q рациональных чисел.

Конечные поля называются *полями Галуа* по имени французского математика Эвариста Галуа (1811–1832).

Далее рассматриваются и используются, как правило, конечные поля.

Порядком поля называется число его элементов. Конечное поле порядка q обозначается $GF(q)$ или F_q.

Пример 2.1 Простейшим полем является поле из двух элементов – поле $GF(2)$. Операции этого поля определяются таблицами, из которых следует, что сложение соответствует булевой функции сложения по модулю 2, а умножение – конъюнкции:

$+$	a	
b	0	1
0	0	1
1	1	0

$\times$	a	
b	0	1
0	0	0
1	0	1

Упражнение 2.1 Постройте таблицы операций поля $GF(5)$.

Мультипликативная группа конечного поля порядка q обозначается $GF(q)^*$ и имеет порядок на единицу меньше порядка поля.

Два поля $F^{(1)}$ и $F^{(2)}$ называются *изоморфными,* если существует биекция $\varphi : F^{(1)} \to F^{(2)}$, сохраняющая операции. Эта биекция и обратная к ней функция φ^{-1} называются *изоморфизмами.*

Упражнение 2.2 Покажите, что фактор-множество Z_p кольца Z целых чисел по модулю простого числа p является полем порядка p и что все конечные поля простого порядка p являются простыми и изоморфны друг другу, то есть такие поля составляют класс всех простых конечных полей.

Понятие поля позволяет вводить и использовать большое разнообразие колец, элементы которых определяются как многочлены

$$f(X) = a_0 + a_1X + a_2X^2 + \dots a_nX^n$$

с коэффициентами a_i из данного поля F. Такие многочлены называются *многочленами над полем* F. Наибольшее число d, такое, что коэффициент $a_d \neq 0$, называется *степенью* многочлена $f(X)$. Если при этом $a_d = 1$, то многочлен степени d называется *нормированным* . Степень многочлена $f(X)$ обозначается $\deg f(X)$. Число ненулевых коэффициентов многочлена будем называть его весом. Степень нулевого многочлена естественно определить как -1. Многочлен степени не более $n-1$ над полем F представим упорядоченным набором $(a_0, a_1, \dots, a_{n-1})$ коэффициентов. (Иногда удобно использовать наборы длины, полученные добавлением старших нулевых элементов $a_i,\ i > \deg(X)$.)

Кольцо многочленов над полем F образуется всеми многочленами над F. Оно обозначается $F[X]$. Операции сложения и умножения кольца $F[X]$ определяются теми же правилами, по которым складываются или перемножаются многочлены над действительным полем.

Операция *сложения* сопоставляет двум многочленам $p_1(X) = \sum_{i=0}^{n-1} a_iX^i$ и $p_2(X) = \sum_{i=0}^{n-1} b_iX^i$, их сумму

$$p_1(X) + p_2(X) = \sum_{i=0}^{n-1} (a_i + b_i)X^i. \qquad (2)$$

(Здесь и ниже в слагаемых формул, подобных формуле в правой части, имеются в виду операции сложения и умножения в поле F).

Результатом операции *умножения* многочленов $p_1(X) = \sum_{i=0}^{n-1} a_i X^i$ и $p_2(X) = \sum_{i=0}^{n-1} b_i X^i$ является многочлен

$$p(X) = p_1(X) \times p_2(X) = \sum_{i=0}^{2n-2} c_i X^i, \tag{3}$$

где $c_i = \sum_{t+l=i} a_t b_l$.

Нулем кольца многочленов является многочлен 0, все коэффициенты которого нулевые, то есть равны аддитивной единице поля. Единицей кольца многочленов является многочлен 1 нулевой степени. Кольцо многочленов не является полем, так как не всякий многочлен имеет обратный к нему элемент кольца.

Упражнение 2.3 Убедитесь, что приведенное описание кольца многочленов соответствует аксиомам кольца.

3 Алгоритм Евклида и его варианты

Элемент a кольца *делит* элемент b (это обозначается $a|b$), если в кольце найдется элемент q такой, что $b = q \times a$. В кольце $a|0$ при любом a, а $0|a$ влечет $a = 0$. В кольце с единицей $1|a$ также при любом a.

Если $a \neq 0$, то в случае $a|b$ упомянутый элемент q, $b = q \times a$, единственный. Он называется *частным* от деления элемента b на элемент a. Если же $a = 0$, то каждый элемент кольца может выступать в роли такого элемента q, и частное от деления элемента b на элемент 0 не определено.

Пример 3.1 Многочлен $g(X)$ *делит* многочлен $f(X)$, что обозначается $g(X)|f(X)$, если существует многочлен $q(X)$ такой, что $f(X) = q(X) \times g(X)$, – результат операции деления многочлена $f(X)$ на многочлен $q(X)$.

Можно определить отношение эквивалентности $\approx$ на множестве элементов кольца: $a \approx b$ тогда и только тогда, когда $a|b$ и $b|a$.

В обозначениях $[a]_\approx$ классов эквивалентности по этому отношению в качестве представителя a класса указывают элемент, выбираемый по известному правилу. Такой представитель будем называть *нормированным* представителем класса.

Например, если R есть кольцо Z целых чисел, то классы содержат один или два элемента, из которых в качестве нормированного представителя принимается неотрицательный элемент. Классы кольца многочленов $F[X]$ над полем F_q

содержат $q-1$ многочлен или единственный (нулевой) многочлен. В качестве представителя ненулевого класса принимается нормированный многочлен (см. стр. 12).

Далее в этом разделе под R понимаются кольцо Z или кольцо $F_q[X]$. Использование общего обозначения позволит нам дать общее описание ряда алгоритмов. Если $b \in [a]_{\approx},\ a \neq 0$, то (поскольку $a|b$ и $b|a$) существует элемент q_b, кольца R такой, что $b = q_b \times a$ и $a = q_b^{-1} \times b = a$, где q_b^{-1} выполняет роль *нормирующего множителя* . Поэтому элемент b кольца R можно описать в виде

$$(q_b, \tilde{b}),\ \text{где } \tilde{b} = a.$$

Если элемент a нормирован, то $q_a = 1,\ \tilde{a} = a$. В этом случае используется сокращенная запись $(1, \tilde{a}) = a$.

Для нуля примем описания $(1, 0) = 0$.

Пример 3.2 Для представления элементов кольца Z целых чисел нормирующий множитель q^{-1} имеет значение 1 или -1 : наряду с положительным элементом a класс $[a]_{\approx} \in Z_{\approx}$ содержит противоположный к нему элемент $-a$ и других элементов не имеет. Элементы a и $-a$ кольца Z представляются записями

(1,< положительный элемент, представляющий класс>).

(–1,< положительный элемент, представляющий класс>).

Нормирующий множитель в представлении элементов кольца многочленов $F_q[X]$ над полем F_q выбирается из числа $q-1$ значений.

Опишем теперь операции кольца с использованием этих представлений элементов. Операция сложения:

$$(q_1, a_1) + (q_2, a_2) = (q, a),$$

где a есть нормированный представитель класса, которому принадлежит $q_1 \times a_1 + q_2 \times a_2$,

$$q = \begin{cases} \frac{q_1 \times a_1 + q_2 \times a_2}{a}, & \text{если } q_1 \times a_1 + q_2 \times a_2 \neq 0, \\ 1 & \text{в остальных случаях.} \end{cases}$$

Операция умножения:

$$(q_1, a_1) \times (q_2, a_1) = \begin{cases} (q_1 \times q_2, a_1 \times a_2), & \text{если } a_1 \times a_2 \neq 0, \\ (1, 0) & \text{в остальных случаях.} \end{cases}$$

С целью унификации описаний алгоритмов на кольцах Z и $F_q[X]$ будем использовать общее обозначение $\preceq$ отношений $|a| \leq |b|$ на кольце Z и $\deg\, a(X) \leq \deg\, b(X)$ на кольце $G_q[X]$ (считая нулевой многочлен многочленом степени -1), элементы $a(X)$ колец $F_q[X]$ будем обозначать упрощенно a. Будем обозначать $a \prec b$, если $a \preceq b$ и не верно, что $b \preceq a$, то $a \prec b$.

Наибольшим общим делителем НОД(x, y) элементов a и b кольца R называется наибольший по отношению $\preceq$ нормированный элемент $e \in R$, такой, что $e|a$ и $e|b$.

Замечание. В соответствии с этим определением НОД(0,0) не существует.

Пример 3.3 В кольце Z НОД$(-6, -4) = 2$.

Заметим, что элемент a кольца относительно элемента b, $b \preceq a, b \neq 0$, можно представить в виде

$$a = q \times b + r,\ r = 0 \text{ или } r \neq 0 \text{ и } r \prec a. \tag{4}$$

В таких представления элементов кольца Z будем дополнительно считать, что q и r неотрицательны.

В частности, такого рода представлением определяется операция *деления с остатком* – представление элемента a кольца относительно элемента $b, b \neq 0$, в виде

$$a = q \times b + r,\ r = 0 \text{ или } r \neq 0 \text{ и } r \prec b, \tag{5}$$

где r есть *остаток от деления элемента a на элемент b*. Его обозначают $a \bmod b$ или $\operatorname{rem}(a, b)$:

$$a = q \times b + a \bmod b = q \times b + \operatorname{rem}(a, b).$$

Возможен и другой выбор элемента q кольца в выражении (4) его можно взять также как sc^j, например, максимальной возможной при условии $r \prec a$ степени некоторого элемента c кольца. Для кольца многочленов можно взять элемент $c = X$ и $j = \deg\, f(X) - \deg\, g(X)$, а для кольца Z можно принять $c = 2$ и число j как разность максимальных номеров единичных позиций в бинарных представлениях чисел a и b.

В каждом частном случае элемент r в выражении (4) получается как значение $r(a, b)$, определенной для частного случая функции $r(x, y)$.

Алгоритм 3.1

ВХОД: Элементы a и b кольца R, $a \neq 0$ или $b \neq 0$.
ВЫХОД: e=НОД(a, b).

1. $u \leftarrow a,\ v \leftarrow b$.
   Если $a = 0$ то $u \leftarrow v,\ v \leftarrow 0$.
2. Пока $v \neq 0$
   2.1 Если $r(u, v) = u$, то $u \leftrightarrow v$.
   2.2. $r \leftarrow r(u, v)$,
   2.3. $u \leftarrow v$, $v \leftarrow r$.
3. $e \leftarrow u$.
4. Если $e \neq 0$, то вернуть e.

Рис. 5: Алгоритм Евклида вычисления НОД(a, b) элементов a и b кольца R.

Таблица 1: Пример применения алгоритма Евклида. НОД(a, b) =НОД$(115, 25) = u^{(4)}$.

i	$u^{(i)}$	$v^{(i)}$	$r^{(i)}$
0	115	25	15
1	25	15	10
2	15	10	5
3	10	5	0
4	5	0	

Теперь можно представить унифицированное описание алгоритма Евклида вычисления НОД(a, b) элементов a и b кольца R – алгоритм 3.1 на рис. 5.

Замечание. Далее в описаниях алгоритмов для упрощения обозначений мы полагаем, что элементы кольца, к которым эти алгоритмы применяются, нормированы.

Утверждение 3.1 *Алгоритм* 3.1 *вычисляет НОД*(a, b) *элементов* a *и* b *кольца* R.

Пример 3.4 Применим алгоритм 3.1 к числам a =115 и $b = 25$. Вычисления представлены в табл. 1, где столбцы соответствуют последовательным шагам алгоритма (нормирующие множители опущены. В этом примере $r = \mathrm{rem}(a, b)$.

Заметим, что для любых не равных 0 одновременно элементов a, b из $R_{\approx}$

Алгоритм 3.2

ВХОД: элементы a и b кольца R, $a \neq 0$ или $b \neq 0$.
ВЫХОД: e=НОД(a, b) и элементы c и d такие, что $ac + bd = e$.

1. $u \leftarrow a,\ v \leftarrow b,$
   Если $a = 0$ то $u \leftarrow v,\ v \leftarrow 0.$
   Если $u \prec v$, то $c_2 \leftarrow 0$, $c_1 \leftarrow 1$, $d_2 \leftarrow 1$, $d_1 \leftarrow 0$.
   иначе $c_2 \leftarrow 1$, $c_1 \leftarrow 0$, $d_2 \leftarrow 0$, $d_1 \leftarrow 1$.
2. $v \neq 0$
   2.1 $r \leftarrow \text{rem}(u, v)$, $q \leftarrow (u - r)/v$,,
   $c \leftarrow c_2 - q \times c_1$;
   $d \leftarrow d_2 - q \times d_1$.
   2.3 $u \leftarrow v$, $v \leftarrow r$,,
   $c_2 \leftarrow c_1$, $c_1 \leftarrow c$;
   $d_2 \leftarrow d_1$, $d_1 \leftarrow d$.
3. $c \leftarrow c_2$, $d \leftarrow d_2$, $e \leftarrow u$ и вернуть (e, c, d).

Рис. 6: Расширенный алгоритм Евклида.

существует пара (c, d) элементов этого множества такая, что имеет место *линейное представление* НОД(a, b)

$$a \times c + b \times d = \text{НОД}(a, b). \tag{6}$$

Вычислить коэффициенты c и d этого представления можно по *расширенному алгоритму Евклида* – алгоритму 3.2 на рис. 6 или 3.3 на рис. 7.

Утверждение 3.2 *Алгоритм 3.2, вычисляет $e =$ НОД(a, b) и элементы c и d, удовлетворяющие тождеству* (6).

Пример 3.5 Применим алгоритм 3.2 к числам 6 и 5. Вычисления представлены в табл. 2. Здесь $r = \text{rem}\ (a, b)$. Получили, $e = 1$, то есть НОД$(5, 6) = 1$. При этом $ca + db = 1 \cdot 6 + (-1) \cdot 5 = 1$.

Алгоритм 3.3

ВХОД: элементы a и b кольца R, $a \neq 0$ или $b \neq 0$.
ВЫХОД: e=НОД(a, b) и элементы c и d такие, что $ac + bd = e$.

1. $u \leftarrow a,\ v \leftarrow b$,
   Если $a = 0$ то $u \leftarrow v,\ v \leftarrow 0$.
   Если $u \prec v$, то $c_2 \leftarrow 0$, $c_1 \leftarrow 1$, $d_2 \leftarrow 1$, $d_1 \leftarrow 0$.
   иначе $c_2 \leftarrow 1$, $c_1 \leftarrow 0$, $d_2 \leftarrow 0$, $d_1 \leftarrow 1$.
2. Пока $v \neq 0$
   2.1 Если $u \prec v$, то
   $u \leftrightarrow v$, $c_1 \leftrightarrow c_2$, $d_1 \leftrightarrow d_2$,
   2.2 $q \leftarrow p^{\deg\ u - \deg\ v}$, $r \leftarrow (u - s \cdot v \cdot q)$,
   [только в кольце Z : если $r < 0$, то $r \leftarrow r + v$].
   Здесь p есть основание системы счисления или многочлен x,
   s – старший разряд числа u
   или старший коэффициент многочлена u.
   $c \leftarrow c_2 - q \times c_1$;
   $d \leftarrow d_2 - q \times d_1$.
   2.3 $u \leftarrow v$, $v \leftarrow r$,
   $c_2 \leftarrow c_1$, $c_1 \leftarrow c$;
   $d_2 \leftarrow d_1$, $d_1 \leftarrow d$.
3. Если $a \prec b$, то $c_2 \leftrightarrow d_2$,
4. $c \leftarrow c_2$, $d \leftarrow d_2$, $e \leftarrow u$ и вернуть (e, c, d).

Рис. 7: Расширенный алгоритм Евклида.

4 Кольцо вычетов по данному модулю

Рассмотрим еще одно отношение на кольце. Отношение эквивалентности $\equiv$ (mod m) на кольце R,

$$a \equiv b \pmod{m} =_{def} m|(a - b),$$

называется *отношением конгруэнтности* [5] *(сравнением) по модулю элемента* $m \in R$. Здесь m – общее обозначение элемента кольца Z и элемента (многочлена) $m(X)$ некоторого кольца $F_q[X]$. При $m = 0$ введенное отношение является

[5] Отношение эквивалентности $\equiv$ на кольце R называется отношением *конгруэнтности* на нем, если оно сохраняет операции кольца, то есть на множестве классов эквивалентности

Таблица 2: Пример применения расширенного алгоритма Евклида. Элементы в представлении (6) суть: НОД(a,b)=НОД$(6,5) = u_2^{(2)} = 1$, $c = c_2^{(2)} = 1$, $d = d_2^{(2)} = -1$.

i	$u^{(i)}$	$v^{(i)}$	$q^{(i)}$	$r^{(i)}$	$c_2^{(i)}$	$c_1^{(i)}$	$d_2^{(i)}$	$d_1^{(i)}$
0	6	5			1	0	0	1
1	5	1	1	1	0	1	1	-1
2	1	0	0	5	1	-5	-1	6

отношением равенства. Классы эквивалентности $[a]_{\equiv \mathrm{mod}\ m}$ называются *классами конгруэнтности (иногда их называют для краткости вычетами) по модулю m*. Сокращенно они обозначаются $[a]_m$. Фактор-множество кольца R по отношению конгруэнтности по модулю элемента m будем обозначать R/m или, в некоторых случаях, R_m. Очевидно, что оно также является кольцом. Множество классов конгруэнтности по модулю m называется *кольцом вычетов по модулю m*.

Примером является рассмотренное в разделе 1 отношение конгруэнтности по модулю m на кольце Z и кольцо вычетов Z_m.

Пример 4.1 На множестве $F[X]$ можно определить отношение конгруэнтности

$$f_1(X) \equiv\ f_2(X)\ (\mathrm{mod\ g(X)}) \iff \mathrm{g(X)|(f_1(X) - f_2(X))},$$

разбивающее кольцо $F[X]$ на классы конгруэнтности $[c(X)]_{\equiv\ \mathrm{mod} g(X)}$ по модулю многочлена $g(X)$. $f(X) \bmod g(X) = c(X)$, если $f(X) \in [c(X)]_{\equiv \mathrm{mod}\ g(X)}$. Множество классов конгруэнтности с операциями, соответствующими операциям сложения и умножения по модулю $g(X)$ их представителей, образуют *кольцо $F[X]/g(X)$ многочленов по модулю многочлена $g(X)$*.

Упражнение 4.1 Покажите, что описанное отношение $\equiv \bmod m$ является отношением конгруэнтности на кольце R и что классы конгруэнтности образуют кольцо с единицей $[1]_m$ и операциями

$$[a]_m \times [b]_m = [a \times b]_m,\ [a]_m + [b]_m = [a + b]_m.$$

Таким образом, если $c \in [a]_m$, то $a \equiv c\ (\mathrm{mod}\ m)$.

операции умножения и сложения таковы, что выполняются тождества

$$[a]_\equiv \times [b]_\equiv = [a \times b]_\equiv,\ [a]_\equiv + [b]_\equiv = [a + b]_\equiv.$$

Элемент a' называется обратным по модулю m элементом по отношению к элементу a, если $[a']_m[a]_m = [1]_m$, то есть $a'a \equiv 1 \pmod{m}$.

Ненулевые элементы $[a]_m$ кольца R_m, имеющие обратные к ним элементы $[a]^{-1}$ (такие, что НОД$([a]_m, [a]_m^{-1}) = [1]_m$), образуют мультипликативную группу R_m^* (множество элементов из R_m, взаимно простых с m).

Упражнение 4.2 Докажите это.

Эта группа совпадает с множеством ненулевых элементов тогда и только тогда, когда m ($m(X)$ в кольце $F_q[X]$) не имеет нормированных делителей, отличных от него самого или 1. Тогда элемент m называется неприводимым (или простым) и кольцо R_m является полем.

Упражнение 4.3 Докажите это.

Далее классы $[a]_m$ для краткости мы обозначаем просто их представителями a, если значение m ясно из контекста.

Пример 4.2 Множество $\{0, 1, 2, 3, 4\}$ с операциями сложения и умножения по модулю 5 является кольцом, множество $\{1, 2, 3, 4\}$ ненулевых элементов которого с операцией умножения по модулю 5 образует мультипликативную группу. Множество $\{0, 1, 2, 3, 4, 5\}$ с операциями сложения и умножения по модулю 6 является кольцом, но множество $\{1, 2, 3, 4, 5\}$ его ненулевых элементов не является мультипликативной группой: элемент $2 \times 3 \bmod m = 0$.

Если посредством расширенного алгоритма Евклида, применительно к паре элементов a и b кольца R, получается $e = 1$, то есть НОД$(a, b) = 1$, то согласно выражению (6) элемент c является обратным по модулю b к элементу a, а элемент d является обратным по модулю a к элементу b.

Пример 4.3 Элемент 5 кольца Z является обратный к самому себе по модулю 6. Действительно, в примере 3.5 получили, что $e = 1$, следовательно элемент $d = -1 \bmod m$ =5 является обратным к 5 по модулю 6. Применяя этот же алгоритм к числам 6 и 4, получим $e = 2$, что свидетельствует об отсутствии элемента, обратного к 4 по модулю 6, и элемента, обратного к 6 по модулю 4.

Элемент $a^{-1} \bmod m$, обратный к заданному элементу a группы R_m^* (если он существует) можно вычислить по расширенному алгоритму Евклида, применяя его к элементам a и m. Тогда операции в линейном представлении (6) можно

Алгоритм 4.1

ВХОД: элемент b кольца R_m, модуль m, $b \prec m$.
ВЫХОД: $e =$ НОД(m, b).
и элемент d такой, что $db \equiv e \pmod{m}$.

1. $d_2 \leftarrow 0$, $d_1 \leftarrow 1$, $u \leftarrow m$, $v \leftarrow b$.
2. Пока $v \neq 0$
   2.2 $r \leftarrow \text{rem}\ (u, v)$, $q \leftarrow (u - r)/v$,
   $d = d_2 - q \times d_1$,
   2.3 $u \leftarrow v$, $v \leftarrow r$,
   $d_2 \leftarrow d_1$, $d_1 \leftarrow d$,
3. $e \leftarrow a$, $d \leftarrow d_2$ и вернуть (e, d).

Рис. 8: Алгоритм Евклида для вычисления обратного элемента по модулю m. Применяются операции кольца R. Если $e \neq 1$, то обратный элемент не существует.

рассматривать как операции в кольце R_m, в связи с чем оно принимает более простую форму
$$ac \equiv e \pmod{m}. \tag{7}$$
Если $e = 1$, то $c = a^{-1} \bmod m$, иначе обратный к элементу a по модулю m элемент не существует.

Но в этом случае не используются значения c, c_1 и c, то есть для инвертирования в кольце можно применить более простую форму расширенного алгоритма Евклида – алгоритм Евклида, представленный на рис. 8 (алгоритм 4.1) или алгоритм 4.2 на рис. 9.

Удивительно, но только в 2000 году одновременно несколькими авторами (например, [5]) было замечено, что с помощью алгоритма Евклида можно сразу выполнять деление, не разлагая процесс на этапы инвертирования и умножения. Действительно, если мы хотим вычислить $s/t \bmod m$, например, в начале работы алгоритма 4.1 на первом шаге полагаем $a = 0$ $b = s$ и $d_1 = t$ (вместо $d_1 = 1$). Тогда вычисляемые (в кольце R_m) во время его работы элементы $d_1^{(i)}, d_2^{(i)}, u^{(i)}, v^{(i)}$, после любого шага алгоритма удовлетворяют соотношениям $d_1^{(i)} t = u^{(i)} s \bmod m, d_2^{(i)} m = 0 \bmod m$. Останавливая этот вариант ал-

Алгоритм 4.2

ВХОД: элемент b кольца R_m, модуль m, $b \prec m$.
ВЫХОД: $e =$ НОД(m, b).
и элемент d такой, что $db \equiv e \pmod m$.

1. $d_2 \leftarrow 0$, $d_1 \leftarrow 1$, $u \leftarrow m$, $v \leftarrow b$.
2. Пока $v \neq 0$
   - 2.1 Если $u \prec v$, то
     $u \leftrightarrow v$,
     $d_2 \leftrightarrow d_1$,
   - 2.2 $q \leftarrow p^{\deg\, u - \deg\, v}$, $r \leftarrow (u - s \cdot v \cdot q)$,
     [только для кольца Z : если $r < 0$, то $r \leftarrow r + v$].

Здесь p есть основание системы счисления или многочлен x,
s – старший разряд числа u
или старший коэффициент многочлена u.
     $d = d_2 - q \times d_1$,
   - 2.3 $u \leftarrow v$, $v \leftarrow r$,
     $d_2 \leftarrow d_1$, $d_1 \leftarrow d$,
3. $e \leftarrow a$, $d \leftarrow d_2$ и вернуть (e, d).

Рис. 9: Алгоритм Евклида для вычисления обратного элемента по модулю m. Применяются операции кольца R. Если $e \neq 1$, то обратный элемент не существует.

горитма, как обычно, когда $u^{(k)} = 1$, (после k-ой итерации) получаем, что $c_2^{(k)} t \equiv u^{(k)} s \equiv s (\mathrm{mod} m)$, откуда $c_2^{(k)} = s/t \bmod m$.

Пример 4.4 Вычислим частное 3/5 в кольце Z_7 (См. табл. 3).

Пример 4.5 В кольце многочленов $F_q[X]$ представление (4) многочлена $f(X)$ относительно многочлена $g(X), g(X) \preceq f(X)$, приобретает вид

$$f(X) = q(X)g(X) + r(X),\ r(X) = 0 \text{ или } r(X) \neq 0 \text{ и } r(X) \prec f(X). \tag{8}$$

В частности, в кольце многочленов определена операция *деления с остатком:* представление многочлена $f(X)$ многочлена $g(X), g(X) \neq 0$, в виде

$$f(X) = q(X)g(X) + r(X),\ r(X) = 0 \text{ или } r(X) \neq 0 \text{ и } r(X) \prec g(X), \tag{9}$$

где $r(X)$ есть остаток от деления многочлена $f(X)$ на многочлен $g(X)$). Его обозначают $f(X) \bmod g(X)$ или $\mathrm{rem}(f(X), g(X))$.

Таблица 3: Деление посредством алгоритма 4.1. Получено $c_2^{(2)}$=4=3/5 mod 7.

i	$u^{(i)}$	$v^{(i)}$	$q^{(i)}$	$r^{(i)}$	$d_2^{(i)}$	$d_1^{(i)}$	e
0	0	3			0	5	
1	3	1	2	1	5	4	
2	1	0	3	0	**4**	0	1

Таблица 4: Применение алгоритма 3.3 для вычисления представления (10) многочленов $a(X) = 1 + X^2 + X^5$ и $b(X) = 1 + X + X^4$ над $GF[2]$. Здесь $q(X) = X^{\deg a(X) - \deg b(X)}$. Многочлены в представлении (10) суть $e(X) = a(X)^{(5)} = 1$. $c(X) = c_2(X)^{(5)} = X + X^2 + X^3$, $d(X) = d_2(X)^{(5)} = 1 + X^2 + X^3 + X^4$

i	$a(X)^{(i)}$	$b(X)^{(i)}$	$q(X)^{(i)}$	$r(X)^{(i)}$	$c_2(X)^{(i)}$	$c_1(X)^{(i)}$	$d_2(X)^{(i)}$	$d_1(X)^{(i)}$
0	101001	11001			1	0	0	1
1	11001	11	01	11	0	1	1	01
2	11	1101	0001	1101	1	0001	01	10001
3	1101	11	001	111	0001	1	10001	01
$3'$	11	111			1	0011	01	10011
4	111	11	01	1	0011	1	10011	01
$4'$	11	1	01	1	1	0111	01	10111
5	1	1	01	1	0111	10111	10111	000111

В другом случае элемент $q(X)$ кольца в выражении (8) можно взять как sX^j, $s \in GF(q)$, например, равным максимальной возможной при условии $r(X) \prec f(X)$ степени X. Показатель этой степени можно получить как $j = \deg f(X) - \deg g(X)$.

В соответствии с тождеством (6) имеет место линейной представление наибольшего общего делителя двух элементов кольца :

$$e(X) = c(X) \times f(X) + d(X) \times g(X). \tag{10}$$

Для вычисления многочленов $e(X)$, $c(X)$ и $d(X)$, удовлетворяющих соотношению (10), можно использовать алгоритм 3.2 или 3.3.

Вычислим по алгоритму 3.3 представление (10) для многочленов $1 + X^2 + X^5$ и $1 + X + X^4$ над $GF[2]$. Вычисления представлены в табл. 4 (ввиду того, что любой элемент кольца $GF(2)[X]$ совпадает с противоположным к нему элементом, в данном случае при вычислениях обозначения знаков элементов не используются).

Полученный многочлен $X+X^2+X^3$ является обратным по модулю многочлена $1+X+X^4$ к многочлену $1 + X^2 + X^5$, а многочлен $1 + X^2 + X^3 + X^4$ является обратным по модулю многочлена $1+X^2+X^5$ к многочлену $1+X+X^4$ в кольце $GF(2)[X]$. Действительно, можно проверить, что

$$((1 + X^2 + X^5)(X + X^2 + X^3)) + ((1 + X^2 + X^3 + X^4)(1 + X + X^4)) = 1.$$

Если операции в тождестве (10) рассматривать как операции в кольце многочленов по модулю многочлена $g(X)$, то оно превратится в тождество

$$e(X) \equiv c(X)f(X)(\mathrm{mod}\ g(X)), \tag{11}$$

и если $e(X) = 1$, то $c(X) = f(X)^{-1}\mathrm{mod}\ g(X)$. Этот многочлен можно вычислить, применяя алгоритм 4.1 или 4.2 при $s = 1$. Вычисления можно свести в таблицу, подобную табл. 4, отличающуюся тем,что отсутствуют столбцы c_1 и c_2. Если же вместо $c_1 = 1$ использовать многочлен $h(X)$, то по этому алгоритму получится многочлен

$$c(X) = h(X)e(X)/f(X)\mathrm{mod}\ g(X).$$

5 Поля Галуа

Теория конечных полей является основой многих разделов всей современной криптографии, в том числе и криптографии эллиптических кривых. Конечные поля используются не только в криптографии, но и в теории кодирования. Благодаря этим своим сферам применения и широкому распространению цифровой техники теория конечных полей превратилось из чистейшей области математики (бывшей некогда предметом исследования Ферма, Эйлера, Лагранжа, Лежандра, Гаусса, Галуа и других выдающихся ученых) в едва ли не прикладной ее раздел. Более того, возможно, именно теория конечных полей в каком-то смысле служит основой самых распространенных в современном мире приложений математики, так как почти каждый человек, если и не посылал зашифрованные с помощью почтовых программ письма, то хотя бы держал в руках мобильный телефон, смотрел телевизор или слушал плеер.

Далее мы излагаем основы теории конечных полей по-возможности самым элементарным образом, не используя общих теорем теории полей, не пользуясь даже теоремой о единственности разложения на неприводимые множители, формулой для числа неприводимых многочленов и теоремой об изоморфизме полей разложения.

6 Характеристика поля

Определение 6.1 *Характеристикой поля* называется наименьшее натуральное число m, такое, что $m * 1 = 0$, или число 0, если такого числа m не существует.

Иными словами, характеристика поля определяется как аддитивный порядок мультипликативной единицы поля.

Следующие факты вытекают из этого определения непосредственно.

Следствие 6.1 *Если p – характеристика поля F, то для любого $a \in F$ выполняется $p * a = 0$.*

Следствие 6.2 *Характеристика конечного поля — простое число .*

Следствие 6.3 *Если p – характеристика поля F, а m, n, k и l – целые числа, то*

(1) $m * 1 = n * 1 \iff m \equiv n \pmod{p}$,
(2) $(m * 1) + (n * 1) = k * 1 \iff m + n \equiv k \pmod{p}$,
(3) $(m * 1) \cdot (n * 1) = l * 1 \iff m \cdot n \equiv l \pmod{p}$.

Следствие 6.4 *Всякое конечное простое поле характеристики p изоморфно кольцу классов конгруэнтности кольца целых чисел по модулю p.*

Следствие 6.5 *Всякое конечное поле характеристики p содержит простое подполе из p элементов.*

В любом поле результат *операции деления* элемента a на ненулевой элемент b определяется как элемент $c = a \cdot b^{-1}$.

Следующее утверждение позволяет существенно упрощать алгоритмы выполнения арифметических операций в конечных полях.

Теорема 6.1 (Тождества Фробениуса) *Пусть H – поле характеристики p; $a, b \in H$. Тогда для любого натурального k*

$$(a + b)^{p^k} = a^{p^k} + b^{p^k},$$

$$(a - b)^{p^k} = a^{p^k} - b^{p^k}.$$

Если $b \neq 0$, то

$$\left(\frac{a}{b}\right)^{p^k} = \frac{a^{p^k}}{b^{p^k}}.$$

Доказательство. При $k = 1$ все члены разложения $(a+b)^p$ по формуле бинома Ньютона, кроме первого a^p и последнего b^p, имеют множитель p и равны 0 по следствию 6.1. Индуктивный переход очевиден. Второе утверждение для нечетного p следует из первого $(a + (-b))^{p^k} = a^{p^k} + (-b)^{p^k} = a^{p^k} - b^{p^k}$, а при $p = 2$ не отличается от первого. Свойство частного проверяется непосредственно по его определению:

$$(a/b)^{p^k} = (a \times b^{-1})^{p^k}\ a^{p^k} \times b^{-p^k} = a^{p^k}/b^{p^k}.$$

Следствие 6.6 *Возведение в степень p^k многочлена над полем характеристики p можно осуществить возведением в степень отдельных членов:*

$$(a_0 + a_1X + \ldots + a_nX^n)^{p^k} = a_0^{p^k} + (a_1X)^{p^k} + \cdots + (a_nX^n)^{p^k}.$$

Пример 6.1 При $p = 2$ получим $(1 + X^2 + X^3)^4 = 1 + X^8 + X^{12}$.

Пусть $f(X)$ есть многочлен над полем F, являющимся подполем поля Q. Элемент $x \in Q$ такой, что $f(x) = 0$, называется *корнем многочлена $f(X)$ в поле Q*.

Следствие 6.7 *Пусть $f(X)$ есть многочлен над полем F характеристики p и x есть корень этого многочлена в поле Q, $F \subseteq Q$, той же характеристики. Тогда при любом натуральном k элемент $x^{p^k} \in Q$ также является корнем этого многочлена.*

Действительно, $f(x^{p^k}) = f(x)^{p^k} = 0$.

7 Мультипликативная группа конечного поля

Порядок мультипликативной группы F_q^* поля F_q равен $q-1$. *Порядок* $\operatorname{ord} a$ *ненулевого элемента a* этого поля определяется как порядок этого же элемента его мультипликативной группы.

Теорема 7.1 *Для ненулевого элемента a поля $F_q = GF(q)$ справедливы следующие утверждения:*

(1) $(\mathrm{ord}\ a) \mid q-1$

(2) $a^{q-1} = 1$

(3) $a^{q-2} = a^{-1}$

(4) *для любого натурального числа n и любого элемента a поля F_q справедливо тождество Ферма $a^{q^n-1} = 1$*

(5) *для любого натурального числа n и любого элемента a поля F_q справедливо тождество Ферма $a^{q^n} = a$.*

Доказательство. Утверждения (1),(2) и (3) непосредственно получаем из следствий 1.1, 1.2 и 1.4. Утверждение (4) вытекает из следствия 1.3, так как $q-1$ делит число $q^n - 1$; пункт (5) следует из пункта (4).

Теорема 7.2 *Если a – ненулевой элемент порядка δ поля F_q, $n, m \in N$, то*

$$a^m = a^n \iff m \equiv n \bmod \delta.$$

Доказательство. По следствию 1.3 $a^{m-n} = 1 \iff \delta \mid (m-n)$. Отсюда следует

Теорема 7.3 *Если a – ненулевой элемент порядка δ поля F_q, то элементы*

$$1, a, a^2, \ldots, a^{\delta-1} \tag{12}$$

поля F_q все различны.

Теорема 7.4 *Если a – ненулевой элемент порядка δ поля F_q, то элементы* (12) *поля F_q суть все корни многочлена $X^\delta - 1$.*

Доказательство. При любом натуральном k, очевидно, $(a^k)^\delta = (a^\delta)^k = 1$. Поэтому перечисленные элементы являются корнями многочлена. Других корней этот многочлен не имеет, так как число этих элементов равно степени многочлена и все они различны.

Из теоремы 1.2 следует

Теорема 7.5 *Если a – ненулевой элемент порядка δ поля, то*

$$\text{ord } a^k = \delta/(\delta, k),$$

в частности, $orda^k = \delta$ тогда и только тогда, когда $(\delta, k) = 1$.

Теорема 7.6 *Если в поле F_q есть элементы порядка δ, то их количество равно $\varphi(\delta)$.*

Доказательство. По теореме 7.5 среди элементов (12) ровно $\varphi(\delta)$ имеют порядок δ.

Лемма 7.1 *Для функции Эйлера справедливо тождество*

$$\sum_{\delta|n} \varphi(\delta) = n.$$

Доказательство. Число всех правильных дробей со знаменателем n равно n, а число несократимых дробей со знаменателем δ равно $\varphi(\delta)$. Так как каждая правильная дробь после сокращения превращается в несократимую, то число правильных дробей будет также равно

$$\sum_{\delta|n} \varphi(\delta).$$

Теорема 7.7 *Если δ – натуральный делитель числа $q-1$, то число элементов порядка δ поля F_q равно $\varphi(\delta)$.*

Доказательство. Обозначим $\psi(\delta)$ число элементов порядка δ поля F_q. По утверждению (1) теоремы 7.1 имеем

$$\sum_{\delta|q-1} \psi(\delta) = q - 1. \tag{13}$$

Используя лемму 7.1 и принимая во внимание (13), имеем

$$\sum_{\delta|q-1} (\varphi(\delta) - \psi(\delta)) = 0. \tag{14}$$

По теореме 7.6 для любого натурального δ имеем $\psi(\delta) \le \varphi(\delta)$, поэтому из (14) следует $\psi(\delta) = \varphi(\delta)$, если $\delta|q-1$.

Следствие 7.1 *Мультипликативная группа конечного поля F_q – циклическая.*

Доказательство. По теореме 7.7 группа F_q^* имеет $\varphi(q-1)$ образующих элементов.

Определение 7.1 Образующий элемент циклической группы F_q^* называется *примитивным элементом* поля F_q и поле F_q содержит $\varphi(q-1)$ примитивных элементов.

Элемент порядка k мультипликативной группы поля называют также *примитивным корнем k-ой степени из* 1. Так, примитивный элемент поля $GF(q)$ есть примитивный корень $q-1$-ой степени из 1. Примитивный элемент простого поля $GF(p)$ называют также *примитивным элементом по модулю p*.

Более подробно о числовых алгоритмических структурах см. [6].

8 Контрольные вопросы

1. Дайте определения группы, кольца и поля.

2. Как возвести элемент группы в степень?

2. Дайте определение порядка элемента группы.

3. Что такое циклическая группа? Какие элементы являются образующими элементами циклической группы.

4. Как вычислить прядок элемента группы?

5. Как найти образующий элемент циклической группы?

6. Как вычислить элемент, обратный по отношению к данному элементу мультипликативной группы?

7. Что позволяет вычислить расширенный алгоритм Евклида?

8. Как вычислить порядок степени элемента группы?

9. Как применить теорему Эйлера для упрощения возведения в большую степень элемента мультипликативной группы?

Литература

1.Нечаев В.И. Элементы криптографии. М.: Высшая школа, 1999.

2.Прахар К. Распределение простых чисел. М.: Мир, 1967.

3.Menezes A.J., van Oorschoft P., Vanstone S.A. Handbook of Applied Cryptography. – CRC Press, Boca Raton, New York, London, Tokio, 1997.

4.Кнут Д. Искусство программирования на ЭВМ, т.2., Вильямс, 2000.

5.Schroeppel R. Automatically solving equations in finite fields. US Patent application No 09/834,363, publication number US2002/0055962 A1.

6. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. – М: Комкнига, 2007.