**Московский государственный технический университет
имени Н.Э. Баумана**

Факультет «Фундаментальные науки»
Кафедра «Математическое моделирование»

А.Н. Канатников

ИЗБРАННЫЕ ЛЕКЦИИ ПО АЛГЕБРЕ

Конспект лекций

Для студентов факультета ФН

Москва
2009

17. КОЛЬЦО МНОГОЧЛЕНОВ

17.1. Определение кольца многочленов

Кольцо многочленов над коммутативным кольцом с 1. Алгебраическая и функциональная точки зрения на понятие многочлена. Многочлены и расширения основного кольца. Алгебраические и трансцендентные элементы кольца. Кольцо многочленов от нескольких переменных. Теорема: если A — целостное кольцо, то и $A[x_1, \ldots, x_n]$ — целостное кольцо. Следствие: $\deg(fg) = \deg f + \deg g$.

Пусть K — коммутативное кольцо с единицей. Многочленом над кольцом K называют выражение вида

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n,$$

в котором a_i, $i = \overline{0, n}$, — элементы кольца K, а x — формальный символ, называемый переменной многочлена.

Многочлен можно рассматривать с разных точек зрения. С ***функциональной точки зрения*** многочлен — это специального вида функция, или, точнее, отображение кольца K в себя, значение которой для данного элемента кольца получается вычислением выражения. Такой подход уже использовался в теории квадратичных форм, когда квадратичная форма также рассматривалась как функция на линейном пространстве.

Однако в теории колец функциональная точка зрения не всегда допустима. Дело в том, что в некоторых кольцах разные многочлены могут задавать одну и ту же функцию. Например, в кольце $\mathbb{Z}_p$ остатков в $\mathbb{Z}$ по модулю p многочлен

$$z(z-1)\ldots(z-p+1)$$

задает функцию, тождественно равную нулю, поскольку при любом значении переменной z значением многочлена является нуль.

С ***алгебраической точки зрения*** многочлен — это просто формальная сумма, полностью определяемая набором коэффициентов. Совокупность многочленов можно ввести аксиоматически как некую алгебраическую систему, например, следующим образом.

Рассмотрим множество K^f последовательностей элементов кольца K, в которых члены последовательности, начиная с некоторого, равны нулю (так называемые ***финитные последовательности***). Самый последний ненулевой член финитной последовательности будем называть ее степенью. Начальному члену последовательности присвоим номер 0. На множестве K^f вводим операции сложения и умножения по следующим правилам. Сложение покомпонентно:

$$\{a_i\} + \{b_i\} = \{a_i + b_i\}.$$

Произведением двух последовательностей $\{a_i\}$ и $\{b_i\}$ назовем последовательность $\{c_i\}$, члены которой вычисляются в соответствии с правилом

$$c_i = a_0 b_i + a_1 b_{i-1} + \ldots + a_i b_0 = \sum_{k=0}^{i} a_k b_{i-k}.$$

Непосредственная проверка аксиом кольца показывает, что с введенными операциями множество K^f является коммутативным кольцом с единицей, причем множество последовательностей, у которых отличен от нуля только начальный член, т.е. последовательностей вида $\{a_0,\ 0,\ 0,\ \ldots\}$ образует в K^f подкольцо, изоморфное кольцу K. В кольце K^f выделим последовательности e_i,

у которых отличен от нуля только один член с номером i, причем этот член равен 1. Нетрудно убедиться в том, что $e_i \cdot e_j = e_{i+j}$ и, следовательно, $e_i = (e_1)^i$. Также легко установить, что

$$\{a_0,\ \ldots,\ a_n,\ 0,\ \ldots\} = a_0e_0 + a_1e_1 + \ldots + a_ne_n.$$

Элемент e_0 является единицей в кольце K^f. Полагая $x = e_1$, заключаем, что $e_i = x^i$. Отождествив каждый элемент $\{a,\ 0,\ 0,\ \}$ с элементом $a \in K$, мы можем записать

$$\{a_0,\ \ldots,\ a_n,\ 0,\ \ldots\} = a_0 + a_1x + \ldots + a_nx^n.$$

Мы построили кольцо, включающее в себя кольцо K (как говорят, ***расширение кольца*** K), каждый элемент которого естественным образом ассоциируется с некторым многочленом. Мы могли бы заявить, что кольцо многочленов и есть построенное нами кольцо K^f, однако формально существуют и другие способы построения, приводящие к аналогичным результатам. Нам следует назвать кольцом многочленов любое расширение кольца K, полученное добавлением одного элемента, изоморфное кольцу K^f. Более общий подход к построению таких расширений такой.

Пусть $\widehat{K}$ — какое-либо расширение кольца K. Выберем некоторый элемент $t \in \widehat{K} \setminus K$ и рассмотрим подкольцо $K[t]$ в $\widehat{K}$, порожденное множеством $K \cup \{t\}$. Нетрудно показать, что каждый элемент $p \in K[t]$ имеет представление

$$p = a_0 + a_1t + \ldots a_nt^n,$$

причем сумме элементов соответствует сумма многочленов, а произведению — произведение многочленов. Таким образом, возникает гомоморфизм φ_t, который финитной последовательности $\{a_0,\ a_1,\ \ldots,\ a_n,\ 0,\ 0,\ \ldots\}$ ставит в соответствие элемент $p = a_0 + a_1t + \ldots a_nt^n$. Очевидно, что этот гомоморфизм является эпиморфизмом (отображением „на“). Если он является изоморфизмом, то мы имеем кольцо $K[t]$, изоморфное кольцу K^f.

Элемент $t \in \widehat{K} \setminus K$ называется ***алгебраическим***, если существует такой многочлен

$$\{a_0,\ a_1,\ \ldots,\ a_n,\ 0,\ 0,\ \ldots\},$$

что выполняется равенство $a_0 + a_1t + \ldots + a_nt^n = 0$. В противном случае элемент t называется ***трансцендентным***. Каждый трансцендентный элемент t порождает кольцо $K[t]$, изоморфное кольцу многочленов K^f.

Пример 17.1. Рассмотрим множество отображений кольца K в себя. С операциями поточечного сложения и умножения, т.е.

$$(f + g)(x) = f(x) + g(x), \quad (fg)(x) = f(x)g(x),$$

множество отображений является коммутативным кольцом с единицей, включающим в себя кольцо K (как постоянные функции). Выбрав в качестве t тождественное отображение, получим подкольцо $K[t]$ функций, порождаемых многочленами над кольцом K. Если K — бесконечное кольцо, а t — бесконечного порядка, то t — трансцендентный элемент. Иначе он является алгебраическим. #

Кольцо $K[x]$ — это кольцо многочленов одной переменной. Аналогично можно ввести кольцо $K[x_1, \ldots, x_n]$ многочленов от n переменных. Непосредственное построение такого кольца, подобное построению K^f, сложное. Однако отметим, что кольцо $K[x_1, \ldots, x_n]$ можно рассматривать как расширение кольца $K[x_1, \ldots, x_{n-1}]$, полученное с помощью переменной x_n. Мы получаем рекуррентное построение колец многочленов с любым числом переменных.

Теорема 17.1. Если K — целостное кольцо, то $K[x_1, x_2, \ldots, x_n]$ — тоже целостное кольцо.

◀ Доказательство строится по индукции по числу переменных многочлена. Достаточно доказать утверждение для $n = 1$. Непосредственно из определения произведения многочленов вытекает, что если

$$p = a_0 + a_1x + \ldots + a_nx^n, \quad q = b_0 + b_1x + \ldots b_mx^m,$$

где $a_n \neq 0$ и $b_m \neq 0$, то

$$pq = a_0b_0 + (a_1b_0 + a_0b_1)x + \ldots + a_nb_mx^{n+m}$$

(все остальные члены финитной последовательности равны нулю). Из условия целостности кольца K заключаем, что $a_nb_m \neq 0$, т.е. многочлен pq отличен от нулевого и, более того, его степени равна сумме степеней сомножителей. ▶

Следствие 17.1. Если K — целостное кольцо, то при перемножении многочленов их степени складываются.

◀ Любой многочлен $p \in K[x_1, \ldots, x_n]$ степени k можно представить в виде

$$p = p_0 + p_1 + \ldots p_k,$$

где многочлен p_i — совокупность слагаемых многочлена p степени i, т.е. ***однородный многочлен порядка*** i. Представив таким же образом другой многочлен q степени m, заключаем, что

$$pq = p_0q_0 + (p_1q_0 + p_0q_1) + \ldots + p_nq_m.$$

Произведение p_nq_m есть однородный многочлен степени $n + m$, отличный от нуля, поскольку в кольце $K[x_1, \ldots, x_n]$ нет делителей нуля. Значит, и призведение pq имеет степень $n + m$. ▶

17.2. Деление с остатком и его свойства

Многочлен одной переменной над полем. 1) $p \vdots q \Rightarrow \deg p \geqslant \deg q$; 2) $p \vdots q$, $q \vdots r \Rightarrow p \vdots r$; 3) $p_1 \vdots q$, $p_2 \vdots q \Rightarrow p_1 \pm p_2 \vdots q$; 4) $p \vdots q \Leftrightarrow pr \vdots qr$. НОД и алгоритм Евклида. Два следствия из алгоритма Евклида. Дальнейшие свойства: 5) $\text{НОД}(pr, qr) = r\,\text{НОД}(p, q)$; 6) r — общий делитель p и $q \Rightarrow$ то $\text{НОД}\left(\frac{p}{r}, \frac{q}{r}\right) = \frac{\text{НОД}(p,q)}{r}$; 7) $pr \vdots q$, $\text{НОД}(r, q) = 1 \Rightarrow p \vdots q$; 8) $\text{НОД}(r, q) = 1 \Rightarrow \text{НОД}(pr, q) = \text{НОД}(p, q)$; 9) $p \vdots q$, $p \vdots r$, $\text{НОД}(q, r) = 1 \Rightarrow p \vdots qr$. НОД трех и более многочленов. НОК двух многочленов. Связь с НОД. НОК трех многочленов.

Рассмотрим кольцо $P[x]$ многочленов над некоторым полем P.

Теорема 17.2. Для любых многочленов p, $q \in P[x]$, $q \neq 0$, существует такая, и притом единственная, пара многочленов α, $\beta \in P[x]$, причем $\deg \beta < \deg q$, что

$$p = \alpha q + \beta. \tag{17.1}$$

◀ Доказательство существования представления (17.1) проводится методом математической индукции по степени многочлена p.

Пусть многочлен

$$q(x) = b_0 + b_1x + \ldots + b_mx^m$$

задан и фиксирован. Если $\deg p < \deg q = m$, то представление (17.1) будет выполняться при $\alpha = 0$, $\beta = p$. Пусть доказано, что представление (17.1) существует для любых многочленов p, степень которых не превышает $k \geqslant m$. Выберем произвольный многочлен

$$p(x) = a_0 + a_1x + \ldots + a_kx^k + a_{k+1}x^{k+1}$$

степени $k+1$. Несложно убедиться в том, что многочлен $\widetilde{p}(x) = p(x) - \frac{a_{k+1}}{b_m}x^{k+1-m}q(x)$ имеет степень не выше k. Поэтому для него имеет место представление (17.1), т.е. $\widetilde{p} = \widetilde{\alpha}q + \widetilde{\beta}$. Но тогда

$$p(x) = \widetilde{p}(x) + \frac{a_{k+1}}{b_m}x^{k+1-m}q(x) = \Big(\frac{a_{k+1}}{b_m}x^{k+1-m} + \widetilde{\alpha}(x)\Big)q(x) + \widetilde{\beta}(x),$$

т.е. имеет место представление (17.1).

Согласно методу математической индукции, любой многочлен p может быть разложен по многочлену q в виде (17.1). Существование представления (17.1) доказано.

Пусть

$$p = \alpha q + \beta = \alpha_1 q + \beta_1.$$

Тогда

$$(\alpha - \alpha_1)q = \beta_1 - \beta.$$

Однако многочлен слева имеет степень не менее $\deg q$, в то время как правая часть имеет степень меньше $\deg q$. Такое равенство возможно только в случае, когда и слева, и справа стоят нулевые многочлены. В этом случае $\alpha = \alpha_1$, $\beta = \beta_1$, т.е. два различных представления совпадают. ►

В представлении (17.1) многочлен α называется ***частным***, а многочлен ***остатком*** от деления многочлена p на многочлен q. Фактически это представление позволяет ввести две операции в кольце многочленов: $p : q = \alpha$ и $p \bmod q = \beta$. Первая операция — вычисление частного при делении многочленов, вторая — вычисление остатка.

Если в представлении (17.1) $\beta = 0$, то говорят, что ***многочлен p делится на многочлен q*** и пишут $p \vdots q$, при этом многочлен q называют ***делителем*** многочлена p, а многочлен p — ***кратным*** многочлена q.

На множестве $P[x]$ всех многочленов возникает отношение делимости. Непосредственно из определения вытекают простейшие свойства этого отношения:

1) $p \vdots q \Rightarrow \deg p \geqslant \deg q$;
2) $p \vdots q$, $q \vdots r \Rightarrow p \vdots r$;
3) $p_1 \vdots q$, $p_2 \vdots q \Rightarrow p_1 \pm p_2 \vdots q$;
4) $p \vdots q \Leftrightarrow pr \vdots qr$.

Второе свойство означает, что рассматриваемое отношение транзитивно. Очевидно, что оно и рефлексивно, но не является симметричным или антисимметричным. Можно утверждать, что если $p \vdots q$, $q \vdots p$, то эти многочлены имеют одинаковую степень и один получается из другого умножением на элемент поля P (многочлен нулевой степени). Если ограничиться многочленами, у которых старший коэффициент равен 1, называемыми ***унитарными многочленами***, то отношение делимости становится антисимметричным, а значит, отношением порядка. Далее говоря о делителях многочленов, мы будем иметь в виду унитарные многочлены.

Среди всех делителей данных многочленов p и q существуют общие делители. Ясно что степень таких делителей не превышает минимальной из степеней p и q. Среди всех общих делителей p и q существует многочлен наивысшей степени. Как следует из дальнейшего изложения, такой многочлен единственный (в классе унитарных многочленов). Он называется ***наибольшим общим делителем*** (НОД) многочленов p и q. Мы обозначим его НОД(p, q).

Для вычисления НОД двух многочленов можно использовать ***алгоритм Евклида***, состоящий в следующим. Делим многочлен p на многочлен q с остатком, получая частное α_0 и остаток β_0. Затем делим q на α_0 с остатком, получая частное α_1 и остаток β_1. Этот процесс последовательного деления в какой-то момент прервется, поскольку на каждом шаге очередной остаток будет иметь степень, меньшую чем предыдущий по крайней мере на единицу. Получим

систему соотношений

$$\begin{aligned} p &= \alpha_0 q + \beta_0, \\ q &= \alpha_1 \beta_0 + \beta_1, \\ \beta_0 &= \alpha_2 \beta_1 + \beta_2, \\ &\cdots\cdots\cdots \\ \beta_{k-2} &= \alpha_k \beta_{k-1} + \beta_k, \\ \beta_{k-1} &= \alpha_{k+1} \beta_k. \end{aligned} \tag{17.2}$$

Из первого соотношения этой системы можно сделать вывод, что пары многочленов p и q, q и β_0 имеют одно и то же множество общих делителей. В самом деле, если r — общий делитель p и q, то в силу равенства $\beta_0 = p - \alpha_0 q$ многочлен r является делителем β_0, а значит, общим делителем пары q и β_0. Если же r — общий делитель пары q и β_0, то в силу равенства $p = \alpha_0 q + \beta_0$, он является делителем p а потому общим делителем пары p и q.

Используя второе, третье и т.д. соотношения системы, заключаем, что все пары многочленов p и q, q и β_0, β_0 и β_1, …, β_{k-1} и β_k имеют одно и то же множество общих делителей. Но из последнего соотношения системы вытекает, что множество общих делителей пары β_{k-1} и β_k — это множество всех делителей многочлена β_k, причем сам многочлен β_k есть общий делитель любой из указанных выше пар наивысшей степени, т.е. $\beta_k = \text{НОД}(p, q)$.

Изложенный алгоритм вычисления НОД позволяет сделать два дополнительных вывода. Во-первых, любой общий делитель пары многочленов p и q является делителем НОД этих многочленов. Во-вторых, верно следующее утверждение.

Теорема 17.3. Если $d = \text{НОД}(p, q)$, то существуют такие многочлены μ и ν, что

$$\mu p + \nu q = d.$$

◄ Запишем для многочленов p и q последовательность делений (17.2). Тогда $\beta_k = \text{НОД}(p, q) = d$. Из предпоследнего равенства (17.2) заключаем, что

$$d = \mu_k \beta_{k-2} + \nu_k \beta_{k-1}, \tag{17.3}$$

где $\mu_k = 1$, $\nu_k = -\alpha_k$.

Второе с конца равенство в системе (17.2) имеет вид $\beta_{k-3} = \alpha_{k-1}\beta_{k-2} + \beta_{k-1}$. Отсюда получаем $\beta_{k-1} = \beta_{k-3} - \alpha_{k-1}\beta_{k-2}$. С помощью этого представления исключим β_{k-1} из равенства (17.3): $d = \nu_k \beta_{k-3} + (\mu_k - \nu_k \alpha_{k-1})\beta_{k-2}$. Следовательно,

$$d = \mu_{k-1}\beta_{k-3} + \nu_{k-1}\beta_{k-2},$$

где $\mu_{k-1} = \nu_k$, $\nu_{k-1} = \mu_k - \nu_k \alpha_{k-1}$. Продолжая процесс последовательного исключения старшего остатка, придем к утверждению теоремы. ►

На основании этих следствий из алгоритма Евклида можно получить дальнейшие свойства отношения делимости:

5) $\text{НОД}(pr, qr) = r\,\text{НОД}(p, q)$;
6) если r — общий делитель p и q, то $\text{НОД}\left(\frac{p}{r}, \frac{q}{r}\right) = \frac{\text{НОД}(p,q)}{r}$;
7) если $pr \vdots q$, $\text{НОД}(r, q) = 1$, то $p \vdots q$;
8) если $\text{НОД}(r, q) = 1$, то $\text{НОД}(pr, q) = \text{НОД}(p, q)$;
9) если $p \vdots q$, $p \vdots r$, $\text{НОД}(q, r) = 1$, то $p \vdots qr$.

◄ Свойство 5 вытекает из следующих соображений. Пусть $d = \text{НОД}(p, q)$, $d' = \text{НОД}(pr, qr)$. Очевидно, что $pr \vdots dr$, $qr \vdots dr$, т.е. dr — общий делитель пары pr и qr, а потому является делителем d'. В силу теоремы 17.3 имеем представление $d = \mu p + \nu q$, откуда $dr = \mu(pr) + \nu(qr)$. Следовательно, любой общий делитель пары pr и qr является делителем многочлена dr. В

частности, $dr \vdots d'$. Таким образом, многочлены d' и dr делятся один на другой. С учетом их унитарности заключаем, что $d' = dr$.

Свойство 6 — переформулировка предыдущего. Действительно, положим $p' = p/r$, $q' = q/r$. Тогда равенство $\text{НОД}\left(\frac{p}{r}, \frac{q}{r}\right) = \frac{\text{НОД}(p,q)}{r}$ можно записать в виде $\text{НОД}(p', q') = \frac{\text{НОД}(p'r, q'r)}{r}$, а это эквивалентно свойству 5.

Свойство 7 вытекает из теоремы 17.3. В самом деле, так как $\text{НОД}(r, q) = 1$, то существуют такие многочлены μ и ν, что $\mu r + \nu q = 1$. Умножив это равенство на p, получим

$$p = \mu pr + \nu qr.$$

В правой части равенства оба слагаемых делятся на q. Значит, и многочлен p делится на q.

Чтобы доказать свойство 8, отметим, что любой общий делитель пары p и q является также общим делителем пары pr и q. Пусть s — общий делитель многочленов pr и q. Обозначим $d = \text{НОД}(r, s)$. Так как $q \vdots s$, то d — общий делитель многочленов r и q, а так как $\text{НОД}(r, q) = 1$, то $d = 1$. Итак, имеем: $\text{НОД}(r, s) = 1$, $pr \vdots s$. Отсюда следует, что $p \vdots s$ и s является общим делителем пары p и q. Мы доказали, что пары p и q, pr и q имеют одно и то же множество делителей. Значит, эти пары имеют один и тот же НОД.

Для доказательства свойства 9 положим $p/q = s$ (это можно в силу отношения $p \vdots q$). Тогда условие $p \vdots r$ можно записать в виде $qs \vdots r$. Отсюда в силу свойства 7 с учетом условия $\text{НОД}(q, r) = 1$ заключаем, что $s \vdots r$. Поэтому $p = qs$ делится на qr. ►

Понятие наибольшего общего делителя двух многочленов без проблем переносится на любое число многочленов. Остановимся на случае трех многочленов. Тройка многочленов p, q, r имеет общие делители (например, 1), причем степень общего делителя не превышает минимальной из степеней трех многочленов. Следовательно, среди общих делителей существует многочлен наивысшей степени. Такой многочлен называется наибольшим общим делителем трех многочленов. Оказывается, вычисление НОД трех (и более) многочленов сводится к последовательному вычислению НОД пар многочленов. Это вытекает из следующей теоремы.

Теорема 17.4. Для любых многочленов p, q, r верно равенство

$$\text{НОД}(p, q, r) = \text{НОД}\big(\text{НОД}(p, q), r\big) = \text{НОД}\big(p, \text{НОД}(q, r)\big).$$

◄ Очевидно, что наибольший общий делитель как функция от трех многочленов не зависит от порядка аргументов. Поэтому в теореме можно ограничиться доказательством только первого равенства. Это равенство будет доказано, если мы установим что тройка многочленов p, q, r и пара многочленов $\text{НОД}(p, q)$ и r имеют одно и то же множество общих делителей.

Если d — общий делитель многочленов p, q, r, то он делится на $\text{НОД}(p, q)$, а следовательно, является общим делителем пары многочленов $\text{НОД}(p, q)$ и r. Пусть d — общий делитель пары $\text{НОД}(p, q)$ и r. Тогда d — делитель $\text{НОД}(p, q)$, а потому является общим делителем многочленов p и q. Значит, он — общий делитель многочленов p, q, r. ►

Любая пара многочленов p и q имеет общие кратные (например pq). Среди всех общих кратных пары p и q существует многочлен наименьшей степени. Он (среди унитарных) единственный. Его называют ***Наименьшим общим кратным*** (НОК) и обозначают $\text{НОК}(p, q)$. Вычисление наименьшего общего кратного двух многочленов сводится к вычислению их наибольшего общего делителя согласно следующей теореме.

Теорема 17.5. Для любых двух многочленов p и q верно равенство

$$\text{НОК}(p, q) = \frac{pq}{\text{НОД}(p, q)}.$$

◄ Обозначим $d = \text{НОД}(p, q)$, $p' = p/d$, $q' = q/d$. Тогда $\frac{pq}{d} = \frac{p'q'd^2}{d} = p'q'd$, и мы видим, что многочлен $s = \frac{pq}{d}$ является общим кратным пары многочленов $p = p'd$ и $q = q'd$.

Покажем, что любое другое общее кратное s' этой пары делится на s. Так как $s' \vdots p$ и $s' \vdots q$, то $s'/d \vdots p'$ и $s'/d \vdots q'$. При этом в силу свойства 6

$$\text{НОД}(p', q') = \text{НОД}\Big(\frac{p}{d}, \frac{q}{d}\Big) = \frac{\text{НОД}(p, q)}{d} = \frac{d}{d} = 1.$$

Следовательно, согласно свойству 9, $s'/d \vdots p'q'$ и $s' \vdots p'q'd$, т.е. $s' \vdots s$. ►

Замечание. Из доказательства теоремы вытекает, что множество всех общих кратных двух многочленов совпадает с множеством всех кратных их НОК.

Как и в случае наитбольшего общего делителя понятие наименьшего общего кратного переносится на любое число многочленов. При этом справедлив следующий аналог теоремы 17.4.

Теорема 17.6. Для любых многочленов p, q, r верно равенство

$$\text{НОК}(p, q, r) = \text{НОК}\big(\text{НОК}(p, q), r\big) = \text{НОК}\big(p, \text{НОК}(q, r)\big).$$

◄ Доказательство этой теоремы является повторением с небольшими изменениями доказательства теоремы 17.4: нужно показать, опираясь на замечание, что множество общих кратных тройки многочленов p, q, r совпадает с множеством общих кратных пары многочленов $\text{НОК}(p, q)$ и r. ►

17.3. Разложение на неприводимые множители

Неприводимые многочлены. Основная теорема. Линейные многочлены и выделение линейных множителей. Кольца $\mathbb{C}[x]$ и $\mathbb{R}[x]$.

17.4. Использование делимости в теории шифрования

Общая постановка задачи шифрования. Шифрующий и дешифрующий ключи. Алгоритм шифрования с открытым ключом.

Теория делимости в множестве целых чисел используется в современных шифровальных системах. Общая задача здесь состоит в том, чтобы по определенному алгоритму закодировать сообщение, преследуя две цели: а) обеспечить защиту информации от несанкционированного доступа; б) гарантировать в дальнейшем восстановление исходного сообщения без каких-либо искажений.

Различают системы шифрования с симметричным и асимметричным ключом. В случае асимметричного ключа используются разные ключи для шифрования сообщения и его дешифрования.

Использование асимметричного ключа повышает возможности защиты от несанкционированного доступа к данным. Есть ряд ситуаций, когда нет необходимости скрывать ключ шифрования, а важно скрыть ключ дешифрования, который не нужно передавать тем, кто формирует сообщения. При таком подходе к шифрованию (шифрованию с открытым ключом) любой может послать сообщение адресату, но прочитать это сообщение может лишь тот, кто имеет ключ дешифрования.

В современных компьютерных системах нашла применение и обратная ситуация, когда закрытым является ключ шифрования, а открытым — ключ дешифрования. Например, в механизмах цифровой подписи зашифрованное сообщение (подпись) доступно любому, но сформировать цифровую подпись может лишь тот, кто обладает ключом шифрования. Разумеется, в этом случае доступ к ключу шифрования позволяет подделать цифровую подпись.

Мы рассмотрим один алгоритм с асимметричным ключом, который можно использовать и для шифрования с открытым ключом, и для дешифрования с открытым ключом.

Алгоритм базируется на паре простых чисел p и q. Полагаем $n = pq$. Выбираем число e, взаимно простое с $m = (p-1)(q-1)$ и не превышающее m. Тогда в кольце вычетов $\mathbb{Z}_m$ число e является обратимым. Полагаем $d = e^{-1}$, где обратный элемент вычисляется в $\mathbb{Z}_m$. Пара чисел n и e составляет ключ шифрования, а пара чисел n и d — ключ дешифрования.

Предположим, что сообщение представляет собой последовательность чисел S_1, S_2, …, S_k, каждое из которых меньше n. Полагаем

$$C_i = S_i^e \bmod n, \quad i = \overline{1,\, k}.$$

Последовательность C_1, C_2, …, C_k представляет собой зашифрованное сообщение. Расшифровывание сообщения осуществляется по формулам

$$S_i = C_i^d \bmod n, \quad i = \overline{1,\, k}.$$

Теорема 17.7. Если НОД$(e, m) = 1$, то e — обратимый элемент в $\mathbb{Z}_m$.

◀ В соответствии с теоремой 17.3 из условия НОД$(e, m) = 1$ вытекает, что для некоторых целых чисел μ и ν выполняется равенство $\mu e + \nu m = 1$. Это равенство в факторкольце $\mathbb{Z}/m\mathbb{Z}$ по идеалу $m\mathbb{Z}$ означает, что $(\mu + \mathbb{Z})(e + \mathbb{Z}) = 1 + \mathbb{Z}$. Указанное факторкольцо изоморфно кольцу $\mathbb{Z}_m$, в котором это равенство трансформируется в следующее: $\mu' e = 1$, где μ' — остаток от деления μ на m. ▶

Теорема 17.8. Если $k - 1 \vdots (p-1)(q-1)$, то $S^k - S \vdots n$.

◀ Утверждение $S^k - S \vdots n$ означает, что если $S \neq 0$, то $S^{k-1} = 1$ в $\mathbb{Z}_n$. Условие $k-1 \vdots (p-1)(q-1)$ равносильно равенству $k - 1 = \alpha(p-1)(q-1)$. Таким образом, утверждение теоремы сводится к следующему: если $0 < S < pq$, то $S^{(p-1)(q-1)} - 1 \vdots pq$. Согласно малой теореме Ферма имеем $S^{p-1} - 1 \vdots p$. Отсюда вытекает, что* $S^{(p-1)(q-1)} - 1 \vdots p$. Аналогично $S^{(p-1)(q-1)} - 1 \vdots q$. Согласно свойству 9 заключаем, что $S^{(p-1)(q-1)} - 1 \vdots pq$. ▶

Предложенная схема может оказаться непригодной, если „официальный“ ключ дешифрования d можно заменить другим „паразитным“, причем таких „паразитных“ окажется много. Задача взломщика упрощается, так как ему для чтения достаточно найти любой из „паразитных“ ключей.

Теорема 17.8 имеет довольно очевидное усиление: если $k-1 \vdots$ НОК$(p-1, q-1)$, то $S^k - S \vdots n$. Отсюда естественный вывод: при подборе чисел p и q желательно, чтобы НОД$(p-1, q-1)$ был как можно меньше.

17.5. Кватернионы

Комплексные числа и $\mathbb{R}^n$ как объект для построения числовой системы. Комплексные числа как действительные матрицы второго порядка вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. Кватеринионы как комплексные матрицы второго порядка. Сложение и умножения — матричные. Множество кватернионов как четырехмерная алгебра над $\mathbb{R}$. Базис этой алгебры. Представление кватернионов в базисе. Таблица базисных произведений. Сопряженный кватернион как эрмитово сопряженная матрица. Вывод отсюда равенства $\overline{z_1 z_2} = \overline{z_2}\,\overline{z_1}$. Норма кватерниона. Тождество $|z| = z\,\overline{z}$. Норма произведения. Свойства операций: а) групповые свойства сложения; а) альтернативность умножения: $ba = \overline{a}\,\overline{b}$; в) ассоциативность; г) нет делителей нуля.

*Опять $S^{p-1} - 1 \vdots p$ означает, что $S^{p-1} = 1$ в $\mathbb{Z}_p$. Но тогда $S^{(p-1)(q-1)} = 1$ в $\mathbb{Z}_p$, что опять-таки эквивалентно отношению $S^{(p-1)(q-1)} - 1 \vdots p$.

ОГЛАВЛЕНИЕ