Лекция №10

18.10.24

8. Решение линейных уравнений и систем линейных уравнений в замкнутом полукольце (продолжение)

Линейные уравнения

Полезно иметь в виду следующее утверждение:

Теорема. Полукольцо является полукольцом с тривиальной итерацией тогда и только тогда, когда единица полукольца есть его наибольший элемент (по естественному порядку).

Доказательство. Достаточность условия очевидна.

Обратно, пусть для любого a его итерация $a^* = 1$, то есть

$$a^* = \sum_{n=0}^{\infty} a^n = \sum_{n=0}^{\infty} (1 + a + \ldots + a^n) = 1 + \sum_{n=1}^{\infty} (a + \ldots + a^n) = 1 + \sum_{n=1}^{\infty} a^n = 1.$$

Отсюда для любого a имеем:

$a \le \sum_{n=1}^{\infty} a^n \le 1$, что и требовалось[1].

Следовательно, все идемпотентные полукольца рассмотренных выше примеров[2], кроме полукольца бинарных отношений, являются полукольцами с тривиальной итерацией. В этом можно убедиться и непосредственным вычислением (см. Учебник, пример 3.5, с. 180-182).

Замечание. Итерация бинарного отношения $\rho \subseteq M^2$ есть

$\rho^* = \bigcup_{n=0}^{\infty} \rho^n = \mathrm{id}M \cup \bigcup_{n=1}^{\infty} \rho^n$ (Учебник, пример 3.5г, с. 182).

Можно показать, что это наименьшее по включению рефлексивное и транзитивное отношение, содержащее ρ. Оно называется *рефлексивно-транзитивным замыканием отношения* ρ. Например, рефлексивно-транзитивное замыкание отношения доминирования, если оно не пусто, будет соответствующее отношение порядка.

Вопрос. Что будет рефлексивно-транзитивным замыканием пустого отношения?

---

[1] Достаточность условия более подробно может доказана так:

$a^* = \sum_{n=0}^{\infty} a^n = \sum_{n=0}^{\infty} (1 + a + \ldots + a^n) = \sum_{n=0}^{\infty} 1 = 1$ (единица поглощает все остальные слагаемые).

[22] Лекция №9.

Пример. Вспомним уравнение относительно неизвестного множества, которое мы решали при обсуждении теоремы о неподвижной точке в индуктивно упорядоченных множествах (лекция №5):

$X = (A \cap X) \cup B$.

Теперь мы с полным основанием можем утверждать, что это уравнение вида (1) в полукольце множеств (см. пример 2 из лекции №9) и, поскольку это полукольцо с тривиальной итерацией, его наименьшее решение есть множество B, что мы получили и на лекции №5 другими способами.

Подчеркнем, что везде в теории линейных уравнений и систем линейных уравнений рассматриваются именно ***наименьшие решения***. Это согласуется и с приложениями рассматриваемой теории к теории графов и формальных языков: в прикладных задачах важны именно наименьшие решения.

Матрицы над полукольцом

Необходимо теперь распространить теорию линейных уравнений на решение систем таких уравнений. Но прежде надо распространить структуру полукольца на множество матриц, элементы которых берутся из некоторого полукольца.

Могут быть определены матрицы любого типа (размера) над некоторым исходным полукольцом. Мы уже фактически работали с такими матрицами, представляя с их помощью конечные соответствия. На самом деле это были матрицы над полукольцом $\mathbf{B}$.

Операции над такими матрицами производятся точно так же, как над числовыми, но только сложение, умножение, нуль и единица понимаются так, как они определены в исходном полукольце, которому принадлежат элементы матриц. Подробно это изложено в Учебнике, п. 3.3.

Пусть $\mathbf{S} = (S, +, \cdot, 0, 1)$ - некоторое полукольцо, не обязательно замкнутое (но обязательно идемпотентное! Напомним, что мы рассматриваем только идемпотентные полукольца).

Обозначим $M_n(S)$ множество квадратных матриц n-го порядка, элементы которых принадлежат полукольцу S. Будем называть их матрицами над полукольцом S. Рассмотрим алгебру $M_n(\mathbf{S}) = (M_n(S), +, \cdot, O, E)$ с операциями матричного сложения и умножения, а также нулевой и единичной матрицами.

Без доказательства сформулируем теорему:

Теорема. Алгебра $M_n(\mathbf{S}) = (M_n(S), +, \cdot, O, E)$ есть полукольцо. Если исходное полукольцо замкнуто, то и полукольцо матриц также замкнуто.

(Доказательство см. в Учебнике, п. 3.3.)

Тогда в замкнутом матричном полукольце можно решать линейные матричные уравнения:

$$X = AX + B \qquad (4)$$

и

$$X = XA + B \qquad (5)$$

Решениями (наименьшими!) этих уравнений будут

$X = A^* B$ и $X = BA^*$ соответственно.

В частности, если матрица $B = E$ (есть единичная матрица), то решения обоих уравнений совпадают и равны итерации матрицы A, то есть $A^* = \sum_{n=0}^{\infty} A^n$.

Но нужно разработать алгоритмы решения таких матричных уравнений. Как мы сейчас увидим, это и будут алгоритмы решения систем линейных уравнений в замкнутых полукольцах.

Решение систем линейных уравнений

Общий вид системы (право)линейных уравнений n-го порядка в замкнутом полукольце $\mathbf{S} = (S, +, \cdot, 0, 1)$:

$$\begin{cases} x_1 = a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n + b_1 \\ x_2 = a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n + b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_n = a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n + b_n \end{cases} \qquad (6)$$

Вводя матрицу $A = (a_{ij})_{n \times n}$, называемую основной матрицей системы (6), векторы-столбцы неизвестных $\xi = (x_1, x_2, \ldots, x_n)^T$ и свободных членов $\beta = (b_1, b_2, \ldots, b_n)^T$, перепишем систему (6) в векторно-матричной форме:

$$\xi = A\xi + \beta \qquad (7)$$

Вернемся теперь к праволинейному матричному уравнению (4). Обозначая ξ_j j-й столбец матрицы X, а через β_j - j-й столбец матрицы B, перепишем матричное уравнение (4) как систему векторно-матричных уравнений относительно столбцов неизвестной матрицы X:

$$\xi_j = A\xi_j + \beta_j, 1 \le j \le n \qquad (8)$$

Пример для матриц 2-го порядка:

$$\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

Для 1-го столбца неизвестной матрицы:

$$\begin{cases} x_{11} = a_{11}x_{11} + a_{12}x_{21} + b_{11} \\ x_{21} = a_{21}x_{11} + a_{22}x_{21} + b_{21} \end{cases}$$

То есть:

$$\begin{pmatrix} x_{11} \\ x_{21} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x_{11} \\ x_{21} \end{pmatrix} + \begin{pmatrix} b_{11} \\ b_{21} \end{pmatrix}$$

Второй столбец расписывается точно так же.

Таким образом, решение матричного уравнения (4) сводится к решению системы векторно-матричных уравнений (8), каждое из которых, расписанное в скалярной форме, есть не что иное, как система (6). Само существование решения матричного уравнения (4) следует из доказанной выше разрешимости линейных уравнений в любом замкнутом полукольце.

Можно строго обосновать[3] алгоритм последовательного исключения неизвестных (аналогичный известному методу Гаусса для числовых линейных систем), позволяющий найти наименьшее решение системы (6).

Из первого уравнения системы исключаем неизвестное x_1, выражая его через остальные слагаемые правой части:

$$x_1 = a_{11}^{*}(a_{12}x_2 + \ldots + a_{1n}x_n + b_1).$$

Во все остальные уравнения подставляем это выражение и после приведения подобных членов получим систему, порядок которой на единицу меньше:

$$x_k = (a_{k1}a^{*}_{11}\,a_{12} + a_{k2})x_2 + \ldots + (a_{k1}a^{*}_{11}\,a_{1k} + a_{kk})x_k + \ldots + \\ + (a_{k1}a^{*}_{11}\,a_{1n} + a_{kn})x_n + (a_{k1}a^{*}_{11}\,b_1 + b_k), k = 2,\ldots,n$$

Так последовательно исключаем все неизвестные и приходим, наконец, к уравнению относительно неизвестного x_n

$$x_n = \alpha_n x_n + \beta_n,$$

где выражения α_n и β_n уже не содержат неизвестных, и значение неизвестного x_n получается в окончательном виде:

$$x_n = \alpha_n^{*}\beta_n.$$

На этот заканчивается «прямой ход» процедуры решения. Далее «обратным ходом» последовательно находим значения всех неизвестных.

---

[3] См. статью Белоусов А.И. О некоторых свойствах полуколец //Машиностроение и компьютерные технологии//2018. - №3 (выложена в облаке).

Покажем это на примере системы 2-го порядка:

$$\begin{cases} x_1 = a_{11}x_1 + a_{12}x_2 + b_1 \\ x_2 = a_{21}x_1 + a_{22}x_2 + b_2 \end{cases}$$

Из первого уравнения выразим x_1:

$$x_1 = a_{11}^*(a_{12}x_2 + b_1).$$

Подставим это во второе уравнение:

$$x_2 = a_{21}a_{11}^*(a_{12}x_2 + b_1) + a_{22}x_2 + b_2,$$
$$x_2 = (a_{21}a_{11}^*a_{12} + a_{22})x_2 + a_{21}a_{11}^*b_1 + b_2$$

Обозначим $\alpha_2 = a_{21}a_{11}^*a_{12} + a_{22}, \beta_2 = a_{21}a_{11}^*b_1 + b_2$ и запишем найденное значение неизвестного $x_2 = \alpha_2^*\beta_2$. Подставляя это в первое уравнение, получим окончательное решение системы.

Процедура сильно упрощается для полуколец с тривиальной итерацией. Все «звездочки» исчезают, и мы получим:

$$x_1 = a_{12}x_2 + b_1, x_2 = a_{21}b_1 + b_2 \Rightarrow x_1 = a_{12}(a_{21}b_1 + b_2) + b_1.$$

См. примеры решения таких систем в семинаре №4.

Такова практика решения и матричных уравнений, и систем линейных уравнений в замкнутых полукольцах.

Замечание. По поводу матричных уравнений: если в уравнении

$$X = AX + B$$

матрицы X и B таковы, что только их первые столбцы отличны от нуля, то записанное выше матричное уравнение станет равносильным уравнению относительно неизвестного вектора ξ - 1-го столбца матрицы X :

$$\xi = A\xi + \beta,$$

где β - первый столбец матрицы B.

То есть примет вид системы (6) или (7).

9. Подгруппы. Теорема Лагранжа

Определение подгруппы

Пусть $\mathbf{G} = (G, \cdot, 1)$ - группа, а $H \subseteq G$ - некоторое подмножество ее носителя.

Это подмножество называется *замкнутым*, если 1) для любых $a,b \in H$ произведение $ab \in H$; 2) для любого $a \in H$ обратный $a^{-1} \in H$; 3) $1 \in H$.

Тогда на множестве $H \subseteq G$ может быть определена группа $\mathbf{H} = (H, \cdot, 1)$. Она называется *подгруппой* группы $\mathbf{G} = (G, \cdot, 1)$.

Например, множество четных целых чисел образует подгруппу аддитивной группы целых чисел, а множество нечетных не образует, так как не является замкнутым. Множество диагональных (а также верхне- и нижнетреугольных) невырожденных матриц образует подгруппу группы всех невырожденных матриц. Множество степеней любого элемента произвольной группы образует подгруппу, а именно, циклическую подгруппу, порожденную этим элементом.

Среди всех подгрупп данной группы выделяют две тривиальные: одна состоит только из единицы, а вторая совпадает со всей группой. Подгруппа, не совпадающая со всей группой, называется *собственной подгруппой*.

Замечание. Понятие подгруппы является частным случаем понятия *подалгебры*, которое мы не рассматриваем (см. Учебник, п. 4.2). Заметим неформально, что по аналогии можно ввести понятие подкольца[4] (и подполукольца), как кольца (полукольца), построенного на подмножестве носителя исходной структуры, которое замкнуто в том же смысле, что и выше, относительно всех операций кольца (или полукольца). Например, кольцо (на самом деле поле) рациональных чисел есть подкольцо (точнее, подполе) кольца (на самом деле, поля) всех действительных чисел. А кольцо целых чисел есть лишь подкольцо (но не подполе) поля рациональных чисел. На множестве невырожденных квадратных матриц нельзя построить подкольцо кольца всех матриц, так нулевая матрица не является невырожденной и сумма двух невырожденных матриц вполне может иметь нулевой определитель (придумайте пример!).

Определение смежных классов

Далее, ради простоты обозначений, будем группу обозначать так же, как и ее носитель.

Пусть G - группа, а H - ее подгруппа (это обозначают так: $H \leq G$[5]; не следует путать это обозначение с обозначением включения, так как не всякое подмножество носителя группы будет носителем ее подгруппы).

Множество $aH = \{ah : h \in H\}$, где $a \in G$ (всей группе!) называется *левым смежным классом подгруппы* H *по элементу* a.

Правый смежный класс есть, по определению, множество $Ha = \{ha : h \in H\}$.

Для коммутативной группы левый и правый смежный классы (для произвольно фиксированного элемента), очевидно, совпадают.

---

[4] См. Учебник, п. 2.6, с. 143-144.

[5] И $H < G$ для собственной подгруппы.

Но в общем случае это не так.

В группе $\mathbf{GL}(2)$ невырожденных квадратных матриц 2-го порядка рассмотрим подгруппу $\mathbf{D}(2)$ диагональных матриц (проверить, что это действительно подгруппа!). Фиксируем произвольно матрицу $A=\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ из группы $\mathbf{GL}(2)$.

Тогда левый смежный класс подгруппы $\mathbf{D}(2)$ по матрице A будет множеством

$$A\mathbf{D}(2)=\left\{\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}: d_1, d_2 \neq 0\right\}=\left\{\begin{pmatrix} a_{11}d_1 & a_{12}d_2 \\ a_{21}d_1 & a_{22}d_2 \end{pmatrix}: d_1, d_2 \neq 0\right\},$$

тогда как правый смежный класс

$$\mathbf{D}(2)A=\left\{\begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}: d_1, d_2 \neq 0\right\}=\left\{\begin{pmatrix} a_{11}d_1 & a_{12}d_1 \\ a_{21}d_2 & a_{22}d_2 \end{pmatrix}: d_1, d_2 \neq 0\right\} \neq A\mathbf{D}(2)$$

Если подгруппа H такова, что для любого a левый и правый смежный классы совпадают, то есть $aH = Ha$, то она называется *нормальной подгруппой*, или *нормальным делителем*.

Ясно, что в коммутативной группе любая подгруппа будет нормальной.

В следующем разделе («Теория графов») мы рассмотрим еще некоторые примеры нормальных делителей (при обсуждении групп автоморфизмов неориентированных графов).

А сейчас перейдем к анализу свойств смежных классов. Речь пойдет только для левых. Для правых все утверждения также будут справедливы.

Свойства смежных классов

Докажем 4 леммы.

Лемма 1. Для любого $h \in H$ $hH = H$. То есть левый смежный класс подгруппы по любому ее элементу совпадает с самой подгруппой.

Доказательство. Для доказательства равенства двух множеств используем метод двух включений.

Пусть $x \in hH$. Тогда $x = hh_1$ для некоторого $h_1 \in H$. Но в силу замкнутости H $x \in H$.

Если же $x \in H$, то можно этот элемент представить так: $x = 1 \cdot x = (hh^{-1})x = h(h^{-1}x) \in hH$, так как $h^{-1}x \in H$.

Итак, $hH = H$.

Лемма2. Для любых $a, b \in G$ $abH = a(bH)$.

Доказательство сразу следует из ассоциативности групповой операции. Эта лемма показывает, как вычислять левый смежный класс по произведению.

Лемма 3. Левые смежные классы образуют разбиение группы, т. е. попарно не пересекаются, и каждый элемент группы принадлежит какому-то из них.

Доказательство. Во-первых, для любого $a \in G$ $a = a \cdot 1 \in aH$, так как $1 \in H$.

Далее, если предположить, что $aH \cap bH \neq \varnothing$ для некоторых $a, b \in G$, то пусть $c \in aH \cap bH$. Тогда для некоторых $h_1, h_2 \in H$ имеем:

$c = ah_1 = bh_2$, откуда

$b = ah_1h_2^{-1}$, и, в силу леммы 2

$bH = (ah_1h_2^{-1})H = (ah_1)(h_2^{-1}H) = (ah_1)H = a(h_1H) = aH$, то есть указанные смежные классы совпадают.

Лемма доказана, то есть левые смежные классы либо совпадают, либо не пересекаются.

Лемма 4. Все левые смежные классы попарно эквивалентны[6] (т. е. находятся во взаимно однозначном соответствии).

Доказательство. Определим отображение $\varphi : H \to aH$ подгруппы H в произвольно фиксированный смежный класс aH следующим образом: $\varphi(h) = ah$. Это отображение сюръективно, так как любой элемент смежного класса aH имеет прообраз h. Но оно и инъективно, так как, если $\varphi(h_1) = \varphi(h_2)$, то есть $ah_1 = ah_2$, то в силу законов сокращения в группе $h_1 = h_2$.

Итак, подгруппа находится во взаимно однозначном соответствии с любым смежным классом. Но тогда и два любых смежных класса находятся между собой во взаимно однозначном соответствии. Действительно, если $\varphi_1 : H \to aH$ и $\varphi_2 : H \to bH$ - две биекции подгруппы на два разных смежных класса, то композиция $\varphi_1^{-1} \circ \varphi_2$ является биекцией смежного класса aH на смежный класс bH : $aH \xrightarrow{\varphi_1^{-1}} H \xrightarrow{\varphi_2} bH$.

Рассмотренные свойства смежных классов, истинные для *любой* группы, для *конечных* групп приводят к очень важному результату, называемому ***теоремой Лагранжа*** для конечных групп.

Теорема. Порядок конечной группы делится на порядок любой ее подгруппы.

Доказательство. В случае конечной группы из лемм 1—4 получаем, что при любой фиксированной подгруппе группа разбивается на одинаковые по числу элементов (левые) смежные классы этой подгруппы, среди которых находится и сама подгруппа. Стало быть, порядок подгруппы одновременно является числом элементов каждого

---

[6] Множества называют эквивалентными (или равномощными), если существует биекция одного на другое.

смежного класса, и ***порядок всей группы равен произведению порядка подгруппы на число смежных классов***: $|G|=k|H|$.

Теорема доказана.

Число k смежных классов данной подгруппы (неважно, левых или правых, так как все полученные выше результаты остаются в силе и для правых смежных классов) называют *индексом подгруппы* H *в группе* G и обозначают $|G:H|$. Тогда можно записать $|G|=|G:H|\cdot|H|$. Образно говоря, всю группу можно уподобить делимому, подгруппу – делителю, а индекс – частному от деления.

Лекция №11

23.10.24

8. Подгруппы. Теорема Лагранжа (продолжение)

Выше (лекция №7) при рассмотрении конечных групп было дано определение порядка элемента a группы G (любой, не обязательно конечной[7]) как наименьшего положительного n, для которого $a^n=1$. Теперь мы можем сказать, что порядок элемента группы равен порядку, порождаемой им циклической подгруппы (уже обязательно конечной!) и, в силу теоремы Лагранжа, в случае конечной группы, является делителем порядка всей группы.

Поэтому получаем:

Следствие. Для конечной группы G и любого ее элемента a имеет место $a^{|G|}=1$.

В частности, для мультипликативной группы вычетов по (простому) модулю *p*: $a^{p-1}=1$,

Откуда заодно получаем формулу для вычисления мультипликативного обратного в поле вычетов: $a^{-1}=a^{p-2}$.

Для примера найдем элемент, обратный в поле $\mathbb{Z}_{31}$ к числу 17.

Имеем: $17^{29}=17^{16}\cdot17^{8}\cdot17^{4}\cdot17$ - разложили 29 по степеням двойки. Вычисляем последовательно квадраты:

$17^2=(-14)^2=14^2=10;17^4=10^2=7;17^8=7^2=18;17^{16}=18^2=(-13)^2=13^2=14.$

Тогда $17^{29}=14\cdot18\cdot7\cdot17=14\cdot(-13)\cdot7\cdot17=14\cdot2\cdot17=(-3)\cdot17=11.$

Легко проверить: $17\cdot11=187=1(\mathrm{mod}\,31)$.

Иногда удается быстро найти порядок элемента, обратный к которому мы ищем и, если он достаточно мал, то показатель степени p-2 надо взять по модулю этого порядка.

---

[7] Пример конечной циклической подгруппы в бесконечной группе – подгруппа поворотов правильного многоугольника, вписанного в окружность. Вся группа в этом случае – группа поворотов окружности (см. Учебник, задача 2.20, с. 165).

Например, в том же поле $25^2 = (-6)^2 = 6^2 = 5; 25^3 = 5 \cdot 25 = 1$, то есть порядок 25 равен 3, и

$25^{29} = 25^{29 \bmod 3} = 25^2 = 5$, что, впрочем, сразу было понятно из равенства $5 \cdot 25 = 1$.

Порядок элемента a конечной группы можно найти, вычислив наименьший положительный показатель степени k такой, что $a^k = -1$. Тогда понятно, что порядок элемента a будет равен $2k$. Но надо быть уверенным в том, что k - ***наименьший*** показатель степени с таким свойством. Если это простое число, то так и есть. В случае составного k это может быть неверно. Например, пусть в группе $\mathbb{Z}_{31}^*$ для некоторого a получилось $a^{15} = -1$. Но $15 = 3 \cdot 5$, и может оказаться, что $a^3 = -1$ или $a^5 = -1$.

Например, в том же поле вычетов по модулю 31 $26^3 = (-5)^3 = -1$, и, конечно, $26^{15} = ((-5)^3)^5 = -1$, но порядок 26 будет равен 6. И, кстати, $26^{-1} = 26^{29 \bmod 6} = 26^5 = (-5)^3(-5)^2 = (-1)(-6) = 6$, что и так понятно из того, что (-5)6=1(mod31).

Проведем те же вычисления для 17.

$17^{15} = 17^{16} \cdot 17^{-1} = 14 \cdot 11 = 154 = -1 (\bmod 31)$, но при этом
$17^3 = 17^2 \cdot 17 = 10 \cdot 17 = 15; 17^5 = 17^3 \cdot 17^2 = 15 \cdot 10 = 26 = -5$.

Отсюда следует, что 15 – наименьший показатель степени, дающий для 17 результат -1.

Значит, порядок 17 равен 30, то есть порядку всей группы $\mathbb{Z}_{31}^*$, и это число есть один из образующих элементов данной циклической группы.

Здесь уместно кое-что сказать вообще об «устройстве» мультипликативных групп вычетов.

Доказывается, что любая такая группа является циклической (доказательство это весьма непросто), причем число ее образующих элементов (называемых также генераторами) определяется формулой:

$\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})...(1 - \frac{1}{p_m}) = n\prod_{k=1}^{m}(1 - \frac{1}{p_k})$, где n - порядок группы и его разложение на простые множители имеет вид: $n = p_1^{k_1} p_2^{k_2} ... p_m^{k_m}$.

Функция $\varphi(n)$ называется функцией Эйлера. Она дает число всех чисел, меньших n и взаимно простых с n.

Замечание. Эту формулу можно вывести из таких соображений.

Если n есть некоторая степень простого числа p, то есть $n = p^k, k \geq 1$, то для получения всех чисел от 1 до n, взаимно простых с n, достаточно из общего

числа всех чисел от 1 до n вычесть число всех чисел, кратных p, которых будет p^{k-1} (включая само число n). То есть

$$\varphi(p^k) = p^k - p^{k-1} = p^k(1-\frac{1}{p}).$$

Нетрудно обобщить это на случай произвольного разложения на простые множители с учетом того, что все множители в разложении попарно взаимно просты.

Для простого числа p получим $\varphi(p) = p(1-\frac{1}{p}) = p-1$.

Часто приходится вычислять функцию Эйлера для числа, представленного в виде произведения попарно различных простых чисел:

$$\varphi(p_1 p_2 ... p_m) = \prod_{k=1}^{m}(p_k - 1).$$

Надо заметить также, что для мультипликативной группы вычетов поля $\mathbb{Z}_p$ число генераторов будет всегда четным (исключая тривиальные случаи $p=2$ и $p=3$), так как образующие элементы всегда ходят парами взаимно обратных[8].

Например, группа $\mathbb{Z}_{31}^*$.

$\varphi(30) = 30(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5}) = 30\cdot\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5} = 8$, то есть 4 пары взаимно обратных генераторов.

Алгоритм вычисления генераторов основан на следующем утверждении:

Если a - образующий элемент конечной циклической группы порядка n, то его степень a^r будет образующим тогда и только тогда, когда число r взаимно просто с n.

Тогда можно подбором найти образующий элемент наименьший в числовом порядке, а затем вычислить его степени, взаимно простые с порядком группы.

Например, для группы $\mathbb{Z}_{31}^*$ наименьший – 3, обратный $21 = 3^{29}$.

Далее:

[8] В любом кольце вычетов по модулю k элемент k-1 обратен сам себе, так как $(k-1)^2 = 1 (\mathrm{mod}\ k)$, и порядок такого элемента будет равен 2. Следовательно он будет образующим только для группы вычетов по модулю 3 (если не учитывать тривиальную группу по модулю 2).

$3^7 = 17, 3^{23} = 3^{-7} = 11;$

$3^{11} = 13, 3^{19} = 3^{-11} = 12;$

$3^{13} = 24, 3^{17} = 3^{-13} = 22.$

То, что 3 является генератором, усматривается из таких вычислений:

$3^{15} = (3^5)^3 = (19 \cdot 3)^3 = (-5)^3 = -1$, но при этом $3^3 = 27 \neq -1$, а $3^5 = -5$.

(См. также семинар №4.)

Некоторые дополнения и приложения

Малая теорема Ферма

В теории чисел есть такая теорема:

Пусть a - целое число, а p - простое число, не являющееся делителем a. Тогда $a^{p-1} = 1 (\mathrm{mod}\ p)$.

◄Разложим число a по модулю p : $mp + r, m \in \mathbb{Z}, r = \mathrm{mod}(a, p)$. По условию $r \neq 0$. Используя формулу бинома Ньютона, получим

$$a^{p-1} = (mp + r)^{p-1} = \sum_{k=0}^{p-1} C_{p-1}^k (mp)^{p-1-k} r^k = r^{p-1} (\mathrm{mod}\ p).$$

Последнее равенство верно, так как все слагаемые записанной выше суммы, кроме последнего, делятся на p.

Но число $r \in \{1, 2, ..., p-1\}$, то есть является элементом группы $\mathbb{Z}_p^*$ и, в силу доказанного выше, $r^{p-1} = 1$ (в этой группе). Отсюда и вытекает утверждение теоремы. ►

Малая теорема Ферма позволяет распознавать делимость очень больших чисел, не прибегая к прямым вычислениям. Например, при $p = 97, a = 102$ $102^{96} - 1 \vdots 97$ (такие примеры можно умножать).

Теорема Эйлера

Малая теорема Ферма допускает обобщение, называемое теоремой Эйлера.

Для любого натурального k и целого a, взаимно простого с k, число $a^{\varphi(k)} = 1$ *(mod k), где* $\varphi(k)$ *– значение определенной выше функции Эйлера для числа k.*

Доказательство аналогично предыдущему и основано на утверждении, что элемент кольца вычетов по модулю k обратим тогда и только тогда, когда он взаимно прост с k (см. в Облаке файл «Решение систем линейных уравнений в кольцах вычетов»). Число $\varphi(k)$ есть не что иное, как порядок группы обратимых элементов указанного кольца. В случае поля $\varphi(k)=k-1$, и мы получаем малую теорему Ферма.

Одна схема кодирования

Можно доказать следующее утверждение:

В кольце $\mathbb{Z}_{pq}$*, где p и q простые числа, для любого* $M \in \{0,1,...pq\}$ *и для любых D и E таких, что* $DE = 1 \bmod (p-1)(q-1)$ $M^{DE} = M \bmod pq$.

◄Если M=0 или M=1, то доказывать нечего. Иначе по теореме Эйлера с учетом того, что $\varphi(pq) = (p-1)(q-1)$, получим $M^{DE} = M^{k(p-1)(q-1)+1} = M^{k\varphi(pq)}M = M \bmod pq$ ►

Этот результат используется при передаче шифрованных сообщений. Цифровой код M кодируется посредством *закрытого ключа* D, т.е. передается код M^D. Получатель, зная число E (*открытый ключ*), декодирует сообщение, возводя полученный код в степень E. При этом отправитель знает также числа p, q, а получатель – число n.

Например: 1) $n = 33 = 3 \cdot 11, D = 3, E = 7; \varphi(n) = 20$.

2) $n = 65 = 5 \cdot 13, \varphi(n) = 48, D = 5, E = 29; DE = 145 = 3 \cdot 48 + 1 = 1 \bmod 48$.

Во втором случае можно было бы положить D=E=7, но это нежелательно, так закрытый и открытый ключи не должны совпадать.

Пусть, например, в первом случае передается число 4, кодирующее, скажем, букву “c” латинского алфавита (первую букву слова computer, которое передается побуквенно). Кодирование состоит в том, что число 4 возводится в куб по модулю 33: $4^3 = -2 = 31$. Получатель должен декодировать сообщение, возведя полученное число в 7-ю степень: $(-2)^7 = 2^6 \cdot (-2) = (-2) \cdot (-2) = 4$.

Конечно, эта схема становится надежной, если числа p, q, D и E достаточно велики.

Числа Ферма

Так называются числа вида $2^{2^n} + 1, n \geq 0$. Ферма думал, что все они простые.

Действительно, как легко проверить, это верно для всех $n \leq 4$, но уже $2^{2^5} + 1 = 2^{32} + 1$ делится на 641. В этом можно убедиться прямым вычислением в мультипликативной группе вычетов по модулю 641. Порядок 2 в этой группе равен, стало быть, 64 (можно проверить, что эта группа циклическая, одним из генераторов которой является число 3).

Можно, однако, доказать такое утверждение:

Если число $2^s + 1$ *простое, то число s есть некоторая степень двойки.*

◄Если число $2^s + 1$ простое, то кольцо вычетов по этому числу (модулю) есть поле, и его мультипликативная группа имеет порядок 2^s, причем $2^s = -1(\bmod(2^s + 1))$. Но в любом кольце вычетов по модулю k единственный, кроме 1, обратный себе самому

элемент есть k-1. Действительно, если предположить, что некоторый элемент $k-\alpha$ обратен сам себе, то $(k-\alpha)^2=\alpha^2=1(\mathrm{mod}\,k)$, откуда $\alpha=\pm1$. Но знак «минус» невозможен, так как получится $k+1\notin\mathbb{Z}_k$. Поэтому $\alpha=1$.Тогда $2^{2s}=2^s\cdot2^s=1$, то есть порядок двойки равен 2s.

(Иначе говоря, s- наименьшее число, для которого $2^s = -1$. Если предположить, что нашлось некоторое $k < s$ такое, что $2^k = -1$, то
$2^k\,2^k = 2^{2k} = (-1)^2=1(\mathrm{mod}\ p)$, и элемент 2^k при $k < s$ был бы сам себе обратен, что невозможно[9].)

По теореме Лагранжа тогда число 2s есть делитель числа 2^s, что и означает, что s является степенью двойки. ►
Доказывается также, что все числа Ферма попарно взаимно просты.

[9] Ну и, очевидно, что не может быть степени $2^k, k<s$, такой, что $2^s\cdot2^k=1$ в силу единственности обратного элемента.