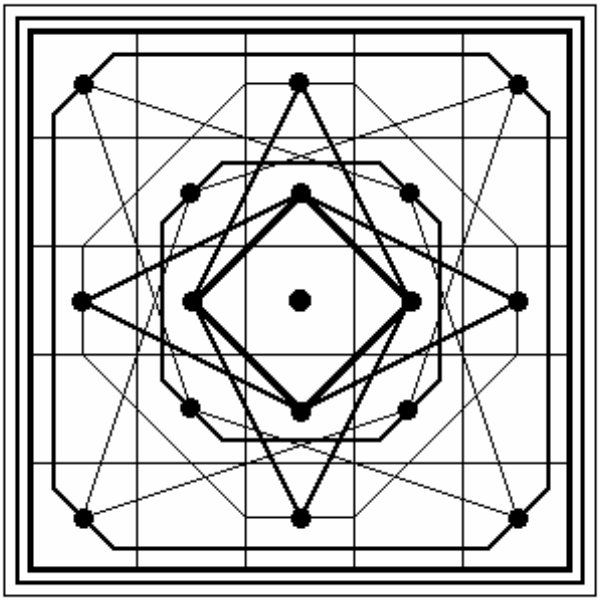
Лекции по Математике. Вып. ТММ-1

Ю. В. Чебраков

ТЕОРИЯ МАГИЧЕСКИХ МАТРИЦ



Санкт-Петербург, 2010

УДК 511+512
ББК 22
Ч345

Р е ц е н з е н т ы:

Доктор физико-математических наук,
профессор С.-Петерб. техн. ун-та
М. А. Салль
Кандидат физико-математических наук,
доцент ин-та истории естествознания и техники РАН
Л. И. Брылевская

Чебраков Ю. В.

Ч345 Теория магических матриц. – СПб.: Изд-во «ВВМ», 2010. – 280 с. – (Лекции по Математике. Вып. ТММ-1.)

ISBN 978–5–9651–0357–7

Данная книга является *первым выпуском* курса лекций, посвященных изложению современного варианта *теории магических матриц* (ТММ). В ней излагаются развитый автором функционально-алгебраический подход к решению различных комбинаторных задач о классических и нетрадиционных магических матрицах (в частности, о классических и нетрадиционных магических квадратах) и основные понятия и методы теории чисел, комбинаторного анализа, теории линейных уравнений и теории матриц, которые наиболее активно используются в ТММ.

Текст лекций написан простым понятным языком, содержит не только теоретический материал, но и описание разнообразных вычислительных алгоритмов и математических методов решения задач.

Книга рассчитана на широкий круг читателей: от студентов вузов и университетов до преподавателей и научных сотрудников.

УДК 511+512
ББК 22

© Ю. В. Чебраков, 2010

ISBN 978–5–9651–0357–7

Глава 2. Линейные уравнения и матрицы

Математические понятия и теоремы существуют независимо от человеческого мышления.
Г. Кантор

2.1. Линейные уравнения с одним и двумя неизвестными

2.1.1. Линейные уравнения с одним неизвестным

А. Уравнение

$$ax - b = 0$$

называется ***линейным уравнением*** с одним неизвестным.

Очевидно, что

указанное уравнение имеет ***единственное*** *решение* $x_0 = b/a$, *когда* $a \neq 0$ *и* $x \in \boldsymbol{R}$.

Б. По аналогии с линейным уравнением определим ***линейное сравнение*** с одним неизвестным (определение и свойства сравнений см. в Разделе 1.2.5):

$$ax - b \equiv 0 \pmod{m}.$$

Рассмотрим, в каких случаях линейное сравнение имеет решение (a, b, m — целые числа).

1) Пусть НОД(a, m) = 1 (a и m являются взаимно простыми числами).

В этом случае, если x принимает последовательно одно из значений

$$0, 1, ..., m - 2, m - 1,$$

то от деления чисел ax на m получим m разных остатков (см. в Разделе 1.3.4 доказательство малой теоремы Ферма) и, следовательно, одно и только одно из чисел ax (например, ax_0) будет сравнимым с числом b по модулю m. Очевидно, что помимо x_0 данному линейному сравнению удовлетворяет и любое x, срав-

нимое с x_0, то есть имеющее вид $x = x_0 + mk$, где k — произвольное целое число.

Таким образом

при НОД(a, m) = 1 *общее решение линейного сравнения имеет вид* $x = x_0 + mk$, *где* $0 \le x_0 \le m - 1$ *и* k — *произвольное целое число.*

Опишем ***три разных способа***, позволяющих найти частное решение x_0 линейного сравнения $ax - b \equiv 0 \pmod{m}$.

Способ 1. Искать x_0 ***методом перебора*** значений 0, 1, ..., $m - 2$, $m - 1$.

Способ 2. В Разделе 1.2.4 приведен алгоритм нахождения таких целых чисел A и B, что $aA + mM$ = НОД(a, m). Так как в нашем случае НОД(a, m) = 1, имеем $aA + mM = 1$. Умножив последнее равенство на b, получим $aAb + mMb = b$, и, значит, справедливо сравнение $aAb - b \equiv 0 \pmod{m}$. Так как исходное сравнение имеет вид $ax - b \equiv 0 \pmod{m}$, приходим к выводу, что $x_0 = Ab$.

Способ 3. В Разделе 1.3.4 доказана теорема Эйлера, согласно которой, если целое число $a > 1$ взаимно просто с m {НОД(a, m) = 1}, то $a^{\varphi(m)} \equiv 1 \pmod{m}$ или

$$a^{\varphi(m)} - 1 \equiv 0 \pmod{m},$$

где $\varphi(m)$ — функция Эйлера, значение которой равно количеству всех таких целых чисел $b < m$, что НОД(b, m) = 1. Умножив последнее сравнение на b, получим, что

$$ba^{\varphi(m)} - b \equiv 0 \pmod{m}.$$

Так как исходное сравнение имеет вид $ax - b \equiv 0 \pmod{m}$, приходим к выводу, что $x_0 = ba^{\varphi(m)-1}$.

П р и м е р 1. Используя Способы 2 и 3, найти решение линейного сравнения

$$105x - 11 \equiv 0 \pmod{38}.$$

i) При использовании Способа 2 имеем

$$105\times(-17) + 38\times47 = 1$$

(см. Пример в Разделе 1.2.4) и, значит, $x_0 = -17\times11 = -187$. Таким образом, общее решение этого сравнения имеет вид

$$x = -187 + 38k$$

или

$$x = -187 + 5\times 38 + 38k = 3 + 38l,$$

где k и l — произвольные целые числа.

ii) При использовании Способа 3 необходимо сначала подсчитать значение функции Эйлера $\varphi(m)$ при $m = 38$. Так как произведение 2×19 является каноническим разложением числа 38, имеем

$$\varphi(38) = (2 - 1)(19 - 1) = 18$$

(способы подсчета значений $\varphi(m)$ см. в Разделе 1.3.4 после доказательства теоремы Эйлера) и, значит, $x_0 = ba^{\varphi(m)-1} = 11\times 105^{17}$. Таким образом, при использовании Способа 3 общее решение обсуждаемого сравнения имеет следующий вид

$$x = 11\times 105^{17} + 38k,$$

где k — произвольное целое число.

Для того чтобы упростить полученное решение, заметим, что

$105 \equiv -9 \pmod{38}$, $\quad 105^2 \equiv 81 \equiv 5 \pmod{38}$,

$105^4 \equiv 25 \pmod{38}$, $\quad 105^5 \equiv -225 \equiv 3 \pmod{38}$,

$105^{15} \equiv 27 \equiv -11 \pmod{38}$, $\quad 105^{17} \equiv -55 \equiv -17 \pmod{38}$,

$$11\times 105^{17} \equiv -187 \equiv 3 \pmod{38},$$

и, значит,

$$x = 3 + 38k.$$

2) Пусть НОД$(a, m) = d > 1$.

В этом случае, $a = da'$, $m = dm'$, где НОД$(a', m') = 1$.

Докажем, что

а) *если b не делится на d нацело, то линейное сравнение не имеет решений*;

б) *если b делится на d, то линейное сравнение имеет d частных решений*

$$x = x_0 + m'k = x_0 - (m/d)k,$$

где $k = 0, 1, 2, \ldots, d - 1$, *а* x_0 *— одно из чисел*

$$0, 1, \ldots, m/d - 1.$$

Действительно,

а) Если x удовлетворяет линейному сравнению $ax - b \equiv 0 \pmod{m}$, то

$$ax - b = mc \text{ и } b = ax - mc = d(a'x - m'c),$$
то есть b должно быть кратно d.

б) Если b делится на d, то $b = db'$ и сравнение $da'x - db' \equiv 0 \pmod{dm'}$ равносильно (см. в Разделе 1.2.5 свойство 3 сравнений) сравнению
$$a'x - b' = 0 \pmod{m'},$$
которое, как уже известно (см. пункт 1), имеет решение
$$x = x_0 + m'k = x_0 - (m/d)k.$$

Легко сообразить, что

α) числа $x_0 + m'k$ образуют столько частных решений исходного сравнения $ax - b \equiv 0 \pmod{m}$, сколько их содержится в полной системе вычетов: 0, 1, 2, ..., $m - 2$, $m - 1$;

β) из чисел $x = x_0 + m'k$ в полную систему наименьших неотрицательных вычетов попадают только
$$x_0, x_0 + m', x_0 + 2m', \ldots, x_0 + (d - 1)m',$$
то есть всего d чисел. Таким образом, у исходного сравнения имеется ровно d частных решений.

П р и м е р 2. Найти все частные решения линейного сравнения
$$9x - 15 \equiv 0 \pmod{21}.$$
Так как НОД(9, 21) = 3 и 15 = 3×5, сравнение $9x - 15 \equiv 0 \pmod{21}$ заменим сравнением
$$3x - 5 \equiv 0 \pmod{7}.$$

i) Используем для решения этого сравнения указанный ранее Способ 2.

Сначала найдем такие целые числа A и B, что $3\times A + 7\times B = 1$ (описание алгоритма нахождения таких целых чисел приведено в Разделе 1.2.4):

1. Из алгоритма Евклида получим следующую цепочку равенств:
$$7 = 3\times 2 + 1$$
$$3 = 1\times 2 + 1$$
$$2 = 1\times 2$$
Откуда НОД(7, 3) = 1, $k = 2$ и набор чисел $\{q\} = 2, 2$.

2. $A_0 = 0$, $B_0 = 1$, $A_1 = 1$, $B_1 = -2$.

$$A_2 = A_0 - q_1 A_1 = 0 - 2\times 1 = -2, \quad B_2 = B_0 - q_1 B_1 = 1 - 2\times(-2) = 5.$$

Таким образом, $A = 5$, $B = -2$ и, значит, справедливо соотношение

$$3\times 5 + 7\times(-2) = 1.$$

Умножив полученное соотношение на 5, получим

$$3\times 5\times 5 + 7\times(-2)\times 5 = 1\times 5.$$

Следовательно, справедливо сравнение

$$3\times 25 - 5 \equiv 0 \pmod 7,$$

а общее решение сравнения $3x - 5 \equiv 0 \pmod 7$ имеет вид

$$x = 25 - 7k \text{ или } x = 25 - 7\times 3 + 7k = 4 + 7l,$$

где k и l — произвольные целые числа.

Все три частных решения исходного сравнения $9x - 15 \equiv 0 \pmod{21}$ получим из общего решения $x = 4 + 7l$ при $l = 0$, 1 и 2:

$$x = 4, 11 \text{ и } 18.$$

ii) Используем для решения сравнения $3x - 5 \equiv 0 \pmod 7$ указанный ранее Способ 3.

Сначала подсчитаем значение функции Эйлера $\varphi(m)$ при $m = 7$. Так как 7 — простое число,

$$\varphi(7) = (7 - 1) = 6$$

(способы подсчета значений $\varphi(m)$ см. в Разделе 1.3.4 после доказательства теоремы Эйлера) и, значит, $x_0 = ba^{\varphi(m)-1} = 5\times 3^5 = 1\,215$. Таким образом, при использовании Способа 3 общее решение обуждаемого сравнения имеет следующий вид

$$x = 1\,215 + 7k = 1\,215 - 173\times 7 + 7k = 4 + 7l,$$

где k и l — произвольные целые числа.

2.1.2. Линейные уравнения с двумя неизвестными

Рассмотрим уравнение

$$ax + by - c = 0,$$

которое называется ***линейным уравнением*** с двумя неизвестными x и y.

1. Очевидно, что

при $a \neq 0$ *и* $x, y \in \boldsymbol{R}$ ($\boldsymbol{R}$ — *множество действительных чисел*) *все решения* x_0 *уравнения* $ax + by - c = 0$ *задаются условиями*

i) $x_0 = (c - by)/a$;

ii) y — *произвольное действительное число.*

2. Пусть $a, b, c, x, y \in \boldsymbol{Z}$, где $\boldsymbol{Z}$ — множество целых чисел. В этом случае уравнение $ax + by - c = 0$ называется ***линейным диофантовым*** уравнением с двумя неизвестными x и y.

а) Если НОД(a, b) = d, то $a = a_1 d$, $b = b_1 d$ и обсуждаемое уравнение имеет вид

$$d(a_1 x + b_1 y) = c .$$

Полученное уравнение может иметь целые решения только в том случае, когда $c = c_1 d$. Сокращая на d, получим уравнение

$$a_1 x + b_1 y = c_1 ,$$

в котором НОД(a_1, b_1) = 1.

Далее будем полагать, что в исходном уравнении $ax + by - c = 0$ НОД(a, b) = 1.

б) Найдем, как выглядит общее решение диофантового уравнения $ax + by - c = 0$.

i) Пусть $c = 0$. В этом случае уравнение имеет вид

$$ax + by = 0$$

и, следовательно,

$$x = -(b/a)\, y.$$

Так как $x, y \in \boldsymbol{Z}$, получаем, что

$$y = ak \text{ и } x = -(b/a)ak = -bk,$$

где k — произвольное целое число.

ii) Пусть $c \neq 0$. Докажем, что

если x_0 *и* y_0 — *частное решение уравнения* $ax + by - c = 0$, *то* ***общее решение*** *этого уравнения имеет вид*

$$x = x_0 - bk, \; y = y_0 + ak.$$

Действительно, пусть x', y' — произвольное решение уравнения $ax + by - c = 0$. Тогда из равенств

$$ax' + by' - c = 0 \text{ и } ax_0 + by_0 - c = 0$$

получаем

$$y' - y_0 = a(x_0 - x')/b.$$

Так как $y' - y_0$ — целое число и НОД(a,b) = 1 получаем, что $x_0 - x'$ должно делиться на b, то есть

$$x_0 - x' = bk, \; y' - y_0 = abk/b = ak,$$

где k — произвольное целое число, и, значит, любое решение x', y' диофантового уравнения $ax + by - c = 0$ имеет вид

$$x' = x_0 - bk, \; y' = ak + y_0.$$

в) Обратим внимание, что из изложенного в пункте (б) не ясно, каким образом можно найти частное решение x_0, y_0 диофантового уравнения $ax + by - c = 0$. В данном пункте продемонстрируем, что для решения указанной проблемы достаточно задачу о решении диофантового уравнения $ax + by - c = 0$, свести к задаче о решении соответствующего линейного сравнения с одним неизвестным.

Действительно, из уравнения $ax + by = c$ получаем, что

$$y = (c - ax)/b.$$

Пусть НОД$(a, c) = d$, то есть $a = a_1 d$ и $c = c_1 d$. Тогда

$$y = (c - ax)/b = (c_1 d - a_1 dx)/b = -d(a_1 x - c_1)/b$$

и, следовательно, должно выполняться линейное сравнение

$$a_1 x - c_1 \equiv 0 \pmod{b}.$$

i) В согласии с указанным ранее Способом 2 решения линейных сравнений (см. Раздел 2.1.1), сравнение $a_1 x - c_1 \equiv 0 \pmod{b}$ имеет целочисленное решение $x = Ac_1 + bk$, где k — произвольное целое число и A — такое целое число, что при некотором целом B справедливо соотношение

$$a_1 A + bB = 1.$$

Умножив соотношение $a_1 A + bB = 1$ на $c_1 d$, получим $a_1 c_1 d A + c_1 d bB = c_1 d$. Откуда, учитывая, что $a_1 d = a$ и $c_1 d = c$, получим соотношение $aAc_1 + b(cB) = c$ и, значит,

$$c - aAc_1 = b(cB).$$

При $x = Ac_1 + bk$

$y = -d(a_1x - c_1)/b = (c - aAc_1)/b - ak = b(cB)/b - ak = cB - ak$

и, очевидно, является целым числом.

Таким образом, получаем следующий результат:

при НОД$(a,b) = 1$ *общее целочисленное решение линейного уравнения* $ax + by - c = 0$ *имеет вид* $x = Ac_1 + bk$ и $y = cB - ak$, *где* k *— произвольное целое число, а* A *и* B *удовлетворяют уравнению* $a_1A + bB = 1$.

ii) В согласии с указанным ранее Способом 3 решения линейных сравнений (см. Раздел 2.1.1), сравнение $a_1x - c_1 \equiv 0 \pmod b$ имеет целочисленное решение $x = c_1a_1^{\varphi(b)-1} + bk$, где k — произвольное целое число и $\varphi(b)$ — функция Эйлера.

При $x = c_1a_1^{\varphi(b)-1} + bk$

$$y = -d(a_1x - c_1)/b = -c(a_1^{\varphi(b)} - 1)/b - ak$$

и так как по теореме Эйлера $(a_1^{\varphi(b)} - 1)$ делится на b (см. Раздел 1.3.4), y является целым числом.

Таким образом, получаем следующий результат:

при НОД$(a,b) = 1$ *общее целочисленное решение линейного уравнения* $ax + by - c = 0$ *имеет вид* $x = c_1a_1^{\varphi(b)-1} + bk$ *и* $y = -c(a_1^{\varphi(b)} - 1)/b - ak$, *где* k *— произвольное целое число и* $\varphi(b)$ *— функция Эйлера*.

Отметим, что для ***упрощения*** указанного решения необходимо

– решение $x = c_1a_1^{\varphi(b)-1} + bk$ представить в виде $x = x_0 + bk$, где $|x_0| < |b|$ (см. Примеры 1, 2 в Разделе 2.1.1);

– решение $y = -c(a_1^{\varphi(b)} - 1)/b - ak$ заменить на $y = y_0 - ak$, где $y_0 = -d(a_1x_0 - c_1)/b$.

П р и м е р. Пусть требуется решить в целых числах уравнение

$$105x + 38y = 5.$$

Имеем $y = (5 - 105x)/38 = -5\times(21x - 1)/38$ и, следовательно, должно выполняться линейное сравнение

$$21x - 1 \equiv 0 \pmod{38}.$$

i) Найдем такие целые числа A и B, что $21\times A + 38\times B = 1$ (описание алгоритма нахождения таких целых чисел приведено в Разделе 1.2.4):

1. Из алгоритма Евклида получим следующую цепочку равенств:

$$38 = 21\times1 + 17$$
$$21 = 17\times1 + 4$$
$$17 = 4\times4 + 1$$
$$4 = 1\times4$$

Следовательно, НОД(38, 21) = 1, $k = 3$ и набор чисел $q_0, q_1, \ldots, q_{k-1} = 1, 1, 4$.

2. $A_0 = 0$, $B_0 = 1$, $A_1 = 1$, $B_1 = -1$. Подсчитаем значения A_{i+1} и B_{i+1} для $i = 1, 2$.

$A_2 = A_0 - q_1A_1 = 0 - 1\times1 = -1$, $\quad B_2 = B_0 - q_1B_1 = 1 - 1\times(-1) = 2$;

$A_3 = A_1 - q_2A_2 = 1 - 4\times(-1) = 5$, $\quad B_3 = B_1 - q_2B_2 = -1 - 4\times2 = -9$.

Таким образом, $A = -9$, $B = 5$ $\{21\times(-9) + 38\times5 = 1\}$, а искомое решение уравнения имеет вид

$$x = Ac_1 + bk = -9\times1 + 38k = -9 + 38k,$$
$$y = cB - ak = 5\times5 - 105k = 25 - 105k,$$

где k — произвольное целое число.

ii) Так как $\varphi(38) = 18$ (см. Пример 1 в Разделе 2.1.1), искомое решение уравнения $105x + 38y = 5$ имеет вид:

$$x = c_1a_1^{\varphi(b)-1} + bk = 21^{17} + 38k,$$

$$y = -c(a_1^{\varphi(b)} - 1)/b - ak = -5(21^{18} - 1)/38 - 105k.$$

Для того чтобы упростить полученное решение, заметим, что

$21 \equiv -17 \pmod{38}$, $\quad 21^2 \equiv 441 \equiv -15 \pmod{38}$,

$21^4 \equiv 225 \equiv -3 \pmod{38}$, $\quad 21^8 \equiv 9 \pmod{38}$,

$21^{16} \equiv 81 \equiv 5 \pmod{38}$, $\quad 21^{17} \equiv -85 \equiv -9 \pmod{38}$.

Откуда получаем, что $x_0 = -9$ и, значит,

$$x = x_0 + bk = -9 + 38k,$$

$$y_0 = -d(a_1x_0 - c_1)/b = -5\times\{21\times(-9)-1)\}/38 = 5\times5 = 25,$$

$$y = y_0 - ak = 25 - 105k,$$

где k — произвольное целое число.

2.2. Классические (магические) и латинские матрицы

2.2.1. Алгоритмы построения классических матриц нечетного порядка

Классической (магической) матрицей {или, как еще часто говорят, классическим (магическим) квадратом} порядка n называется квадратная таблица размера $n\times n$, так заполненная последовательными натуральными числами от 1 до n^2, что их сумма по строкам, столбцам и диагоналям таблицы одинакова. С древних времен известны алгоритмические описания следующих трех простых методов построения классических (магических) матриц нечетного порядка.

А. ***Метод террас***.

Y									
4					5				
3				4		10			
2			3		9		15		
1		2		8		14		20	
0	1		7		13		19		25
–1		6		12		18		24	
–2			11		17		23		
–3				16		22			
–4					21				
X	–4	–3	–2	–1	0	1	2	3	4

(1)

3	16	9	22	15
20	8	21	14	2
7	25	13	1	19
24	12	5	18	6
11	4	17	10	23

(2)

Рис. 5. Построение классической матрицы 5×5 методом террас.