Решение уравнений в кольцах вычетов

Утверждение1. *В любом конечном кольце следующие условия равносильны: 1) элемент не является односторонним делителем нуля, 2) элемент односторонне обратим, 3) элемент обратим, 4) элемент не является делителем нуля.*

◆ Пусть в конечном кольце $\boldsymbol{R}$=(R, +, •, 0, 1) элемент a не является левым делителем нуля, т.е. не существует такого ненулевого b, для которого $a \bullet b = 0$. Определим отображение f_a множества всех ненулевых элементов кольца так, что $f_a(x)=ax$ (левый сдвиг на элемент a). Это отображение инъективно, так как из равенства $ax=ay$ следует $a(x-y)=0$, а так как a не есть левый делитель нуля, то $x-y=0$, т.е. $x=y$. Так как кольцо конечно, то левый сдвиг есть биекция множества его ненулевых элементов, т.е. для любого ненулевого y найдется единственный x такой, что $y=ax$. В частности, при $y=1$ получим $ax=1$, откуда следует, что $x=a^{\mathrm{R}}$ – правый обратный к a.

Докажем, что отсюда следует, что элемент a не является правым делителем нуля. Предполагая противное, получим, что для некоторого ненулевого b выполняется $ba=0$. С другой стороны, $aa^{\mathrm{R}}=1$. Умножая последнее равенство слева на b, получим $(ba)a^{\mathrm{R}}=b=0$, что противоречит определению элемента b. Итак, a не является правым делителем нуля. Тогда, вводя отображение правого сдвига g_a так, что для всякого ненулевого x $g_a(x)=xa$, совершенно аналогично предыдущему докажем, что правый сдвиг – биекция множества всех ненулевых элементов кольца, откуда получим, что для некоторого единственного x' имеет место $x'a=1$, т.е. $x'=a^{\mathrm{L}}$ – левый обратный к a. Легко показать, что односторонние обратные к a совпадают. Действительно, $a^{\mathrm{L}}= a^{\mathrm{L}}1= a^{\mathrm{L}}(aa^{\mathrm{R}})= (a^{\mathrm{L}}a)a^{\mathrm{R}}=1a^{\mathrm{R}}= a^{\mathrm{R}}$. Это значит, что элемент a обратим, т.е. $a^{\mathrm{L}}= a^{\mathrm{R}} = a^{-1}$.

Точно так же обратимость элемента конечного кольца доказывается, если исходить из условия, что он не является правым делителем нуля: доказывается, что он левообратим (через построение правого сдвига), затем – не является левым делителем нуля, затем – правообратим (через построение левого сдвига).

Итак, доказана цепочка 1) ⇒ 2) ⇒ 3).

Доказательство цепочки 3) ⇒ 4) ⇒ 1). Импликация 3) ⇒ 4) доказывается так: если элемент а обратим, то имеем, в частности:
$a^{-1}a = 1$. Если предположить, что a – делитель нуля, то он – и левый и правый делитель нуля[1]. Тогда найдется такой ненулевой элемент x, что $ax=0$. Тогда имеем: $(a^{-1}a)x = a^{-1}(ax) = 0$, т.е. $x = 0$, что невозможно. Значит, a не есть делитель нуля. Тогда он не есть либо левый, либо правый делитель нуля, т.е. имеет место импликация 4) ⇒ 1).♦

Утверждение 2. *В кольце вычетов* $\mathbf{Z}_k$ *элемент обратим тогда и только тогда, когда он взаимно прост с* k.

---

[1] Напомним, что ненулевой элемент кольца называется делителем нуля, если он и левый, и правый делитель нуля одновременно (см. XIX, 173).

♦ Докажем, что элемент не является делителем нуля в $\mathbf{Z}_k$ тогда и только тогда, когда он взаимно прост с k. Пусть элемент a и число k имеют НОД, больший единицы, т.е. для некоторого $m > 1$ и некоторых натуральных l и n выполняется $a=lm$, $k=nm$. Тогда $nm=0$ (mod k) и $an=lmn=0$ (mod k), т.е. a – делитель нуля.

Теперь докажем обратное: пусть НОД(a, k)=1. Предположим, что a – делитель нуля. Тогда найдется такое $m \in \mathbf{Z}_k$, что $am=0$ (mod k), т.е. $am=sk$ для некоторого натурального s. Отсюда $s=am/k$. Стоящая справа дробь есть целое число, что возможно лишь при следующих трех условиях: (1) a делится на k, (2) m делится на k, (3) существуют числа k_1, k_2, большие единицы и меньшие k, такие, что первое есть делитель a, второе – делитель m, и $k_1\, k_2 = k$. Поскольку a и k – взаимно простые числа, то первая и третья альтернативы отпадают, но вторая невозможна, так как $m < k$. Итак, получено противоречие, что и доказывает, что a не является делителем нуля и обратим.

Другое доказательство: если НОД(a, k)=1, то для некоторых x и y ax+ky=1, т.е. ax=1(mod k), и x – обратный к a. Наоборот, пусть a обратим и при этом НОД(a,k)=m>1. Но тогда, как показано выше, a является делителем нуля в $\mathbf{Z}_k$ и не может быть обратимым.♦

Утверждение 3. Уравнение $ax=b$ в кольце Z_m разрешимо тогда и только тогда, когда НОД(a, m)|b, причем тогда уравнение имеет s = НОД(a, m) решений, наименьшее из которых (по естественному числовому порядку) совпадает решением (единственным) уравнения $rx=d$ в кольце Z_l, где $r=a/s, d=b/s, l=m/s.$

♦ *Необходимость условия*: пусть уравнение $ax=b$ в кольце Z_m разрешимо. Это значит, что в кольце целых чисел выполняется равенство $ax-km=b$ для некоторого натурального числа k. Так как при s = НОД(a, m) $a=rs, m=ls$, то имеет место равенство $rsx-kls=b$. Разделив это равенство на s, получим $rx-kl=b/s$, что может иметь место для целых чисел лишь при делимости b на s.

Достаточность условия: при условии делимости b на s, обозначая частное от деления через d, получим уравнение в кольце целых чисел: $rx-kl=d$, откуда получаем уравнение $rx=d$ в кольце Z_l. Но числа r и l взаимно просты. Действительно, иначе было бы для некоторого $p > 1$ и некоторых натуральных x и y: $r=px, l=py$, откуда $a=pxs, m=pys$, и НОД(a, m) $\geq ps > s$, что противоречит соотношению s = НОД(a, m). Следовательно, элемент r обратим в кольце Z_l, и уравнение $rx=d$ в кольце Z_l имеет единственное решение в виде $x=r^{-1}d$.

Рассмотрим теперь числа вида $y = r^{-1}d + \alpha l$ для некоторых натуральных α. Подставляя y в выражение $rsx - kls$ вместо x, будем иметь $rs(r^{-1}d + \alpha l) - kls = rsx + rs\alpha l - kls = ax + m(r\alpha - k) = ax(\mathrm{mod}\, m)$.То есть $rsy - kls = ay - km = ay(\mathrm{mod}\, m) = ax(\mathrm{mod}\, m) = b$, и $y = r^{-1}d + \alpha l$ есть решение уравнения $ax = b$ в кольце Z_m. В то же время понятно, что должно выполняться неравенство $y < m$, откуда следует, что число α может принимать значения от 0 до s–1.

Действительно, рассмотрим сумму $y = r^{-1}d + (s-1)l = r^{-1}d + sl - l = r^{-1}d + m - l$. Но $r^{-1}d$ есть решение уравнения $rx = d$ в кольце Z_l и, следовательно, строго меньше l. Тогда $y = r^{-1}d + m - l < m$, так как $r^{-1}d - l < 0$. Значит, $y = r^{-1}d + \alpha l < m$ при наибольшем значении $\alpha = s - 1$. Подавно и для всех меньших значений, начиная с нуля. Но при $\alpha = s$ получим $r^{-1}d + sl = r^{-1}d + m > m$.

Заметим, что при выполнении условия доказанной теоремы исходное уравнение можно привести умножением его левой и правой частей на m/s (по $\mathrm{mod}\, m$) к виду $0x = 0(\mathrm{mod}\, m)$. В противном же случае получим $0x = b'(\mathrm{mod}\, m)$, $b' \neq 0(\mathrm{mod}\, m)$, что указывает на отсутствие решений. ♦

Из утверждения 3 можно получить следующий результат для целых чисел: *если число* $s = НОД(a,b)$, *то для некоторых целых* x *и* y *выполняется:* $ax + by = s$.

Действительно, если $s = НОД(a,b)$, то уравнение $ax = s(\mathrm{mod}\, b)$ разрешимо, и существует целое y, для которого $ax + by = s$.

В частности, если числа a и b взаимно просты, то есть s=1, то уравнение $ax = 1(\mathrm{mod}\, b)$ *однозначно* разрешимо, и по найденному x легко найти (единственный) y. Поэтому для взаимно простых чисел a и b однозначно определены такие числа x и y, что $ax + by = 1$.

Имеет место также утверждение, более слабое, чем обратное к доказанному. Действительно, пусть указанные числа x и y существуют. Тогда уравнение $ax = s(\mathrm{mod}\, b)$ разрешимо, откуда $НОД(a,b) \mid s$. Обозначая $d = НОД(a,b)$, получим: $a = kd, b = ld, s = md$ для некоторых целых k, l, m. Итак, число s кратно наибольшему общему делителю чисел a и b.

Некоторые примеры

1) В кольце $\mathbb{Z}_{21}$ решить уравнение

$9x = 15$.

Уравнение разрешимо, так как $НОД(9,15) = 3 \mid 21$.

Переходим, как описано выше, к уравнению в кольце (поле) $\mathbb{Z}_7$:

$3x = 5$.

Получаем $x = 3^{-1} \cdot 5 = 5 \cdot 5 = 4$.

Еще два решения (всех решений 3!): 4+7=11 и 4+14=18. Все решения легко проверить.

2) В кольце $\mathbb{Z}_{21}$ решить систему:

$$\begin{cases} 5x + 2y = 1 \\ y - 11x = 13 \end{cases}$$

(Учебник, задача 2.19).

Решение

Из второго уравнения выразим *y*:

$y = 13 + 11x$

и, подставив в первое, получим:

$5x + 2(13 + 11x) = 1,$

$6x = -4 = 17$

Это уравнение не имеет решения, так как $НОД(6, 21) = 3$ не делит 17.

Изменим исходную систему:

$$\begin{cases} 5x + 2y = 1 \\ y + 11x = 13 \end{cases}$$

Тогда

$y = 13 - 11x,$

$5x + 2(13 - 11x) = 1,$

$4x = 17.$

Это уравнение имеет единственное решение, так как числа 4 и 21 взаимно просты, и 4 обратимо: $4^{-1} = -5 = 16$.

Тогда

$x = 16 \cdot 17 = (-5)(-4) = -1 = 20$.

$y = 13 - 11(-1) = 3$.

Проверка:

$$\begin{cases} 5 \cdot 20 + 2 \cdot 3 = 1 \\ 3 + 11(-1) = -8 = 13 \end{cases}$$

3) В кольце $\mathbb{Z}_{18}$ решить систему:

$$\begin{cases} 2x + 10y = 4 \\ 7x - 6y = 4 \end{cases}$$

Рассмотрим два способа решения этой системы.

1 способ.

Умножив первое уравнение на 7, а второе на 2, получим:

$$\begin{cases} 14x + 16y = 10 \\ 14x - 12y = 8 \end{cases}$$

Вычитая из первого уравнения второе, будем иметь:

$10y = 2$.

Это уравнение разрешимо, так как НОД(10, 18)=2, и имеет два решения.

Первое (наименьшее в обычном числовом порядке) есть решение уравнения

$$5y = 1$$

в кольце $\mathbb{Z}_9$:

$y_1 = 5^{-1} = 2$.

Второе решение получается прибавлением к первому числа 9 (частного от деления исходного модуля 18 на НОД(10, 18)=2):

$y_2 = 11$.

Соответствующие решения для *x* получим следующим образом:

$$2x + 10 \cdot 2 = 4,$$
$$2x = -16 = 2.$$

Снова переходя в $\mathbb{Z}_9$, получим $x = 1$ и (уже в исходном кольце) $x = 10$.

Для решения $y_2 = 11$ аналогично:

$$2x + 10 \cdot 11 = 4,$$
$$2x = -106 (\mathrm{mod}\, 18) = 2.$$

Как видно, получим те же решения.

Необходимо сделать проверку, так как умножение уравнения на делитель нуля (в данном случае на 2, второе уравнение) может дать «паразитные» решения.

Легко убедиться в том, что пары (1, 2) и (1, 11) не удовлетворяют системе, так как

$$7 \cdot 1 - 6 \cdot 2 = -5 \neq 4,$$
$$7 \cdot 1 - 6 \cdot 11 = -5 \neq 4.$$

Являются решениями пары (10, 2) и (10, 11):

$$2\cdot 10+10\cdot 2=4,$$
$$7\cdot 10-6\cdot 2=4.$$

и

$$2\cdot 10+10\cdot 11=4,$$
$$7\cdot 10-6\cdot 11=4.$$

Все вычисления выполняем по модулю 18.

2 способ.

Пользуясь тем, что 7 обратимо в $\mathbb{Z}_{18}$, решим второе уравнение относительно x:

$$x=7^{-1}(6y+4)=13(6y+4)=6y-2.$$

Подставляя это в первое уравнение, получим:

$$2(6y-2)+10y=4,$$
$$4y=8$$

Это уравнение разрешимо в силу того, что НОД(4, 18) = 2|8, и имеет два решения, разность между которыми равна 9.

Чтобы получить первое решение, переходим в $\mathbb{Z}_9$, решая уравнение

$2y=4$, откуда $y=5\cdot 4=2$.

Второе решение (как и выше) есть y=11.

Тогда для x получим:

x = 6y-2 = 6·2-2=10,

x = 6y-2 = 6·11-2=10.

Как видно, «паразитного» значения x=1 здесь не получилось.

4) В кольце $\mathbb{Z}_{18}$ решить систему:

$$\begin{cases} 5x+7y=4 \\ 11x-13y=6 \end{cases}$$

Снова решим систему двумя способами.

1 способ.

Умножая первое уравнение на 11, а второе на 5, получим систему

$$\begin{cases} x+5y=8 \\ x-11y=12 \end{cases}$$

и, вычитая затем из первого уравнения второе, получим

$$16y=-4=14.$$

Это уравнение разрешимо, так как НОД(16, 18)=2 | 14.
Переходя в кольцо $\mathbb{Z}_9$, получим уравнение
$8y = 7$, откуда первое решение
$y_1 = 8^{-1} \cdot 7 = 8 \cdot 7 = 2$.
Второе решение $y_2 = 2 + 9 = 11$.
Следовательно,
$x_1 = 8 - 5 \cdot 2 = -2 = 16,$
$x_1 = 8 - 5 \cdot 11 = 7.$
Выполним проверку (подставляя решения в исходную систему):

$$\begin{cases} 5(-2) + 7 \cdot 2 = 4 \\ 11(-2) - 13 \cdot 2 = 14 - 8 = 6 \end{cases}$$

и

$$\begin{cases} 5 \cdot 7 + 7 \cdot 11 = -1 + 5 = 4 \\ 11 \cdot 7 - 13 \cdot 11 = 5 - 13(-7) = 5 + 1 = 6. \end{cases}$$

Как видно, «паразитных» решений тут не получилось. Можно заметить, что в исходной системе все коэффициенты при неизвестных обратимы.

2 способ.
Исключим x из первого уравнения:
$x = 5^{-1}(4 - 7y) = 11(4 - 7y) = 8 - 5y$.
Подставляя это во второе уравнение, получим:
$11(8 - 5y) - 13y = 6,$
$4y = 8,$
Откуда легко получаем (аналогично предыдущему) два решения для y: 2 и 11. Соответственно, для x, как и выше – 16 и 7.

5) В кольце $\mathbb{Z}_{18}$ решить систему:

$$\begin{cases} 6x + 2y = 9 \\ 3x - 8y = 6 \end{cases}$$

Умножая 2-е уравнение на 2 и вычитая из первого, получим:

$$18y = 0 \cdot y = -3 = 15,$$

откуда следует, что решений нет.
Тот же результат можно получить, умножая второе уравнение на 4 и складывая с первым:

$$18x = 0 \cdot x - 12y = -3 = 15,$$
$$12y = 3.$$

Это уравнение неразрешимо, так как НОД(12, 18)=6 не делит 3.

Можно показать, что, решая систему в кольце вычетов по составному модулю методом последовательного исключения неизвестных, получим на некотором шаге вывод о несовместности системы, либо получим некоторые решения, среди которых могут быть «паразитные», то есть удовлетворяющие отдельным уравнениям, но не удовлетворяющие системе в целом. Поэтому все найденные решения необходимо проверить.