Используемые сокращения

ССПС — система сравнений первой степени, она же — система линейных сравнений (в англоязычных статьях встречаются формулировки: [set of] simultaneous linear congruences, system of linear congruence equations, sequence of congruences of the first degree…).

МПП — метод последовательной подстановки (successive substitution method).

КТО — китайская теорема об остатках (Chinese remainder theorem).

Теория

Рассмотрим ССПС

$$\begin{cases} x \equiv b_1 \left(\operatorname{mod} m_1\right) \\ \ldots \\ x \equiv b_T \left(\operatorname{mod} m_T\right) \end{cases}. \tag{1}$$

Она имеет решения тогда и только тогда, когда $НОД\left(m_i, m_j\right)$ делит $\left(b_i - b_j\right)$ (или, что то же самое, $b_i \equiv b_j \left(\operatorname{mod} НОД\left(m_i, m_j\right)\right)$) для всех $1 \le i < j \le T$. В этом случае любые два решения отличаются на величину, кратную $M = НОК\left(m_1, \ldots, m_T\right)$.

Следствие: если все модули попарно взаимно просты ($НОД\left(m_i, m_j\right)=1$ для всех $1 \le i < j \le T$), то система (1) имеет решения при любых значениях b_i. Решения отличаются на величину, кратную $M = m_1 \cdot \ldots \cdot m_T$.

Универсальным методом решения ССПС является МПП. Если все модули попарно взаимно просты, можно также применять алгоритм, основанный на КТО.

Пример 1: система из двух сравнений

$$\begin{cases} x \equiv 2 \pmod 6 \\ x \equiv 5 \pmod 9 \end{cases}.$$

$НОД(6,9)=3$, $2 \equiv 5 \pmod 3$ — значит, решения существуют.

Поскольку $НОД(6,9) \ne 1$, КТО неприменима, и решать нужно с помощью МПП.

МПП

Выразим *x* из первого сравнения: $x = 2 + 6a$, где $a \in \mathbb{Z}$.

Подставим полученное выражение во второе сравнение и решим сравнение относительно *a*:

$$\begin{aligned} x &\equiv 5 \pmod 9 \\ 2+6a &\equiv 5 \pmod 9 \\ 6a &\equiv 3 \pmod 9 \,\big|\, :3 \\ 2a &\equiv 1 \pmod 3 \\ a &\equiv 2 \pmod 3 \end{aligned}$$

Значит, $a = 2 + 3z$, $z \in \mathbb{Z}$.

Подставив это выражение в *x*, получим

$$x = 2 + 6a = 2 + 6 \cdot (2 + 3z) = 14 + 18z.$$

Ответ

$$x = 14 + 18z,\ z \in \mathbb{Z}.$$

// Альтернативный способ записи: $x \equiv 14 \pmod{18}$.

Проверка

$НОК(6,9)=18$ — модуль определён верно.

Подставим $x=14$ в первое сравнение. $14\equiv 2\pmod 6$ — верно, т. к. $(14-2)\vdots 6$.

Подставим $x=14$ во второе сравнение. $14\equiv 5\pmod 9$ — верно, т. к. $(14-5)\vdots 9$.

Замечание

Решение сравнений обязательно нужно доводить до конца, даже если кажется, что промежуточный результат уже можно подставить обратно в x.

Например, если $x=2+6a$, а второе сравнение свелось к виду $2a\equiv 1\pmod 3$, казалось бы, отсюда следует, что $2a=1+3z$ и можно подставить это выражение в x — $x=2+6a=2+3\cdot 2a=2+3\cdot(1+3z)=5+9z$, но на самом деле полученный x удовлетворяет только второму сравнению, а не первому.

Итак, всегда нужно выражать неизвестные в явном виде, без всяких сомножителей. В данном случае — $a\equiv 2\pmod 3$, откуда $a=2+3z$ и т. д.

Пример 2: несовместная система из двух сравнений

Решим систему

$$\begin{cases} x\equiv 2\pmod 6 \\ x\equiv 4\pmod 9 \end{cases}.$$

$НОД(6,9)=3$, $(2-4)$ не делится на 3 — значит, решений нет.

Убедимся в этом, попытавшись решить систему через МПП.

МПП

Выразим x из первого сравнения: $x=2+6a$, где $a\in\mathbb{Z}$.

Подставим полученное выражение во второе сравнение и решим сравнение относительно a:

$$x\equiv 4\pmod 9$$
$$2+6a\equiv 4\pmod 9$$
$$6a\equiv 2\pmod 9$$

Если рассмотреть коэффициент при неизвестном a и модуль, то $НОД(6,9)=3$, однако свободный член 2 не делится на 3. Значит, сравнение $6a\equiv 2\pmod 9$ не имеет решений. В самом деле, условие $6a = 2 + 9q \Leftrightarrow 3 \cdot (2a - 3q) = 2$ невыполнимо для целых значений a и q.

Ответ

Решений нет.

Пример 3: система из трёх сравнений

$$\begin{cases} x \equiv 6 \pmod 8 \\ x \equiv 5 \pmod{13} \\ x \equiv 3 \pmod{15} \end{cases}.$$

Все модули (8 и 13; 8 и 15; 13 и 15) попарно взаимно просты — значит, решения существуют независимо от того, как соотносятся b_i (т. е. числа 6, 5 и 3).

Способ 1: МПП

Выражаем x из первого сравнения, подставляем во второе, решаем, преобразовываем x с учётом этого решения, подставляем новый x в третье — и так пока не дойдём до конца.

Из первого сравнения: $x = 6 + 8a$, $a \in \mathbb{Z}$.

Подставляем x во второе сравнение:

$$x \equiv 5 \pmod{13}$$

$$6 + 8a \equiv 5 \pmod{13}$$

$$8a \equiv 12 \pmod{13}$$

Можно ли сократить обе части на 4? Поскольку $НОД(4,13) = 1$, то существует $4^{-1} \pmod{13}$ (оно равно 10, но это не имеет значения), а значит, обе части сравнения можно домножить на 4^{-1} — по сути, разделить на 4. Получаем $2a \equiv 3 \pmod{13}$.

Любым удобным способом (включая простой подбор) находим, что $a \equiv 8 \pmod{13}$.

Итак, $a = 8 + 13b$, $b \in \mathbb{Z}$.

Тогда $x = 6 + 8a = 6 + 8 \cdot (8 + 13b) = 70 + 104b$.

Подставляем этот x в третье сравнение:

$$x \equiv 3 \pmod{15}$$
$$70 + 104b \equiv 3 \pmod{15}$$
$$-b \equiv 8 \pmod{15}$$
$$b \equiv 7 \pmod{15}$$

Итак, $b = 7 + 15z$, $z \in \mathbb{Z}$.

Тогда $x = 70 + 104b = 70 + 104 \cdot (7 + 15z) = 798 + 1560z$.

Способ 2: КТО

Поскольку все модули попарно взаимно просты, можно воспользоваться алгоритмом, основанным на китайской теореме об остатках.

1. Находим модуль: $M = m_1 \cdot m_2 \cdot m_3 = 8 \cdot 13 \cdot 15 = 1560$.

2. Вычисляем вспомогательные параметры:

$$n_1 = \frac{M}{m_1} = m_2 \cdot m_3 = 13 \cdot 15 = 195,$$

$$n_2 = \frac{M}{m_2} = m_1 \cdot m_3 = 8 \cdot 15 = 120,$$

$$n_3 = \frac{M}{m_3} = m_1 \cdot m_2 = 8 \cdot 13 = 104.$$

3. Находим соотношения Безу $k_i n_i + s_i m_i = 1$ для всех пар (n_i, m_i) расширенным алгоритмом Евклида либо подбором:

$$\underline{3} \cdot 195 + \underline{-73} \cdot 8 = 1, \qquad \underline{-4} \cdot 120 + \underline{37} \cdot 13 = 1, \qquad \underline{-1} \cdot 104 + \underline{7} \cdot 15 = 1.$$

4. Частное решение:

$$x_0 = \sum_{i=1}^{3} b_i k_i n_i \pmod{M} =$$
$$= 6 \cdot (3 \cdot 195) + 5 \cdot (-4 \cdot 120) + 3 \cdot (-1 \cdot 104) \pmod{1560} =$$
$$= 3510 - 2400 - 312 \pmod{1560} = 798.$$

5. Общее решение: $x \equiv 798 \pmod{1560}$.

Ответ

$$x = 798 + 1560z, \ z \in \mathbb{Z}.$$

// Альтернативный способ записи: $x \equiv 798 \pmod{1560}$.

Проверка

$НОК(8,13,15)=8\cdot13\cdot15=1560$ — модуль определён верно.

Подставим $x=798$ в первое сравнение. $798\equiv6(\mathrm{mod}\,8)$ — верно, т. к. $792 \vdots 8$.

Подставим $x=798$ во второе сравнение. $798\equiv5(\mathrm{mod}\,13)$ — верно, т. к. $793 \vdots 13$.

Подставим $x=798$ в третье сравнение. $798\equiv3(\mathrm{mod}\,15)$ — верно, т. к. $795 \vdots 15$.

Пример 4: система из четырёх сравнений с коэффициентами при *x*

$$\begin{cases}7x\equiv1(\mathrm{mod}\,9)\\3x\equiv12(\mathrm{mod}\,14)\\x\equiv1(\mathrm{mod}\,15)\\7x\equiv12(\mathrm{mod}\,20)\end{cases}.$$

Первым делом нужно решить каждое из сравнений в отдельности, то есть привести каждую строку к виду $x\equiv b_i(\mathrm{mod}\,m_i)$.

$7x\equiv1(\mathrm{mod}\,9)$ — подбором определяем, что подходит $x=4$, т. е. $x\equiv4(\mathrm{mod}\,9)$.

$3x\equiv12(\mathrm{mod}\,14)$ — поскольку $НОД(3,14)=1$, то существует $3^{-1}(\mathrm{mod}\,14)$ (оно равно 5, но это не имеет значения), а значит, обе части сравнения можно домножить на 3^{-1} — по сути, разделить на 3. Получаем $x\equiv4(\mathrm{mod}\,14)$.

$x\equiv1(\mathrm{mod}\,15)$ — сравнение уже имеет требуемый вид.

$7x\equiv12(\mathrm{mod}\,20)$ — заметим, что $7\cdot3=21$, а значит, $7^{-1}(\mathrm{mod}\,20)=3$ (можно было также воспользоваться расширенным алгоритмом Евклида). Умножив обе части сравнения на 3, получим $x\equiv16(\mathrm{mod}\,20)$.

Получилась система

$$\begin{cases}x\equiv4(\mathrm{mod}\,9)\\x\equiv4(\mathrm{mod}\,14)\\x\equiv1(\mathrm{mod}\,15)\\x\equiv16(\mathrm{mod}\,20)\end{cases}.$$

Первые два сравнения эквивалентны выражениям $x-4=9k_1$ и $x-4=14k_2$, соответственно. Их можно объединить, заменив модули в правой части на $НОК(9,14)$, получится $x-4=126k$.

$$\begin{cases} x\equiv 4(\bmod 126) \\ x\equiv 1(\bmod 15) \\ x\equiv 16(\bmod 20) \end{cases}.$$

Проверим совместность системы.

$НОД(126,15)=3$. $(4-1)\vdots 3$.

$НОД(126,20)=2$. $(4-16)\vdots 2$.

$НОД(15,20)=5$. $(1-16)\vdots 5$.

Итак, решения есть.

Поскольку среди модулей имеются такие, которые не являются попарно взаимно простыми (строго говоря, они все не являются), КТО неприменима, и решать нужно методом последовательной подстановки.

МПП

Берём сравнение по самому большому модулю — первое. (Выбор обусловлен тем, что большое число, будучи подставленным в сравнение по маленькому модулю, хорошо сократится, а с маленькими числами проще работать.)

$x=4+126a$, $a\in\mathbb{Z}$.

Подставляем x во второе сравнение.

$$x\equiv 1(\bmod 15)$$
$$4+126a\equiv 1(\bmod 15)$$
$$6a\equiv 12(\bmod 15)\,\big|:3$$
$$2a\equiv 4(\bmod 5)\,\big|\times 2^{-1}$$
$$a\equiv 2(\bmod 5)$$

Итак, $a=2+5b$, $b\in\mathbb{Z}$.

Тогда $x=4+126a=4+126\cdot(2+5b)=256+630b$.

Подставляем новый x в третье сравнение.

$$x \equiv 16 \pmod{20}$$
$$256 + 630b \equiv 16 \pmod{20}$$
$$10b \equiv 0 \pmod{20} \,\Big|\, :10$$
$$b \equiv 0 \pmod{2}$$

Итак, $b = 2z$, $z \in \mathbb{Z}$.

Тогда $x = 256 + 630b = 256 + 630 \cdot (2z) = 256 + 1260z$.

Ответ

$$x = 256 + 1260z, \ z \in \mathbb{Z}.$$

// Альтернативный способ записи: $x \equiv 256 \pmod{1260}$.

Проверка

Проверяем исходную систему, то есть

$$\begin{cases} 7x \equiv 1 \pmod{9} \\ 3x \equiv 12 \pmod{14} \\ x \equiv 1 \pmod{15} \\ 7x \equiv 12 \pmod{20} \end{cases}.$$

Подставляем $x = 256$ во все четыре сравнения.

$(7 \cdot 256 - 1) = 1791$, делится на 9.

$(3 \cdot 256 - 12) = 756$, делится на 14.

$(256 - 1) = 255$, делится на 15.

$(7 \cdot 256 - 12) = 1780$, делится на 20.

Всё верно.

Замечание

Следует отметить, что НОК модулей нужно определять не из исходной системы, содержащей множители при *x*, а из системы, приведённой к виду (1). В данном случае $НОК(9,14,15,20) = 2^2 \cdot 3^2 \cdot 5 \cdot 7 = 1260$ — модуль правильный. Но могло получиться и иначе. Например, глядя на ССПС

$$\begin{cases} 2x \equiv 4 \pmod{12} \\ x \equiv 5 \pmod{9} \end{cases},$$

можно ошибочно подумать, что решения системы будут сравнимы по модулю $НОК(12,9) = 36$, однако первое сравнение сокращается на 2 ($x \equiv 2 \pmod{6}$), и на самом деле в ответе будет модуль 18 (см. пример 1).