



Гильмуллин, М. Ф. Китайская Теорема об Остатках (Chinese Remainder Theorem) // Математика с Мансур-абый. 2026. URL: <https://history-math.org/ru/publications/hm-tt-dd2ef8a97500-ru/>. Дата публикации: 05.02.2026.

ОЧЕРК

Китайская Теорема об Остатках (Chinese Remainder Theorem)

Есть такая легенда.

Мансур Гильмуллин · 05.02.2026 · RU

[Статья на сайте журнала](#)



Знаменитая китайская «Терракотовая армия». Иллюстрация к легенде о военных построениях · [Источник](#)

Есть такая легенда.

В древнем Китае военачальники якобы действовали так: отдавали несколько последовательных команд вроде «В колонну по 7 становись!», «В колонну по 11 становись!» и т. д., и в каждом случае смотрели, сколько воинов оказалось в последнем ряду. После этого — только по найденным остаткам — вычисляли общее число солдат.

Алгоритм решения подобных задач в математической литературе называется «китайская теорема об остатках» (Chinese Remainder Theorem). Часто пишут кратко: КТО.

Смысл теоремы очень красив: она позволяет восстановить целое число по набору его остатков при делении на несколько чисел, если эти числа попарно взаимно просты. Это один из классических результатов теории чисел, который давно вышел за пределы «чистой математики» и нашёл применение в компьютерной алгебре и криптографии.

Историческая справка

В арифметической форме эта идея описана в трактате, известном как «Сунь-цзы суаньцзин» (Sunzi Suanjing), который традиционно относят к ранней эпохе (обычно упоминают III век н. э.). В XIII веке китайский математик Цинь Цзюшао существенно обобщил эти методы в книге «Математические рассуждения в девяти главах» (1247), где дал уже систематический алгоритм решения подобных задач.

Задача из книги Сунь Цзы

«Предположим, что имеется неизвестное количество объектов. Разбив их на тройки, получаем в остатке 2; разбив на пятёрки — 3; разбив на семёрки — 2. Сколько имеется объектов?»

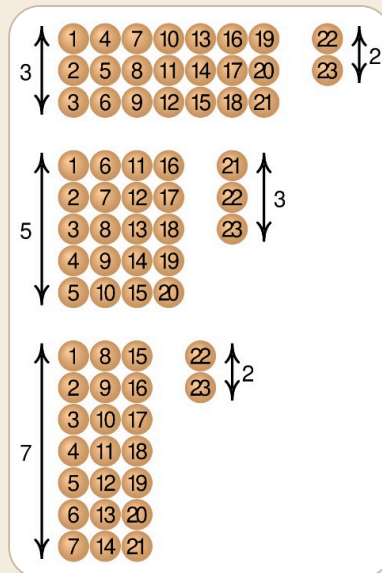
После решения этой конкретной задачи в тексте приводится алгоритм для общего случая (при произвольных остатках):

«Умножь число остатков при делении на тройки на 70, добавь к полученному произведению числа остатков при делении на пятёрки на 21, и затем добавь произведение числа остатков при делении на семёрки на 15. Если результат равен 106 или более — вычти кратное 105».

Проверим на наших данных:

$$2 \cdot 70 + 3 \cdot 21 + 2 \cdot 15 = 233 = 105 \cdot 2 + 23$$

Значит, наименьшее решение — 23.



Пояснение к задаче, решённой по алгоритму Сунь Цзы: $2 \cdot 70 + 3 \cdot 21 + 2 \cdot 15 = 233$ · [Источник](#)

Почему здесь появляются числа 70, 21 и 15? Это не магия: на современном языке математики это частичные произведения и обратные к ним по модулю — они и есть те «кирпичики», из которых строится общий алгоритм.

Два элементарных объяснения

1 способ (комбинаторный)

Выпишем множества решений трёх отдельных условий (достаточно смотреть числа до $3 \cdot 5 \cdot 7 = 105$):

$x \equiv 2 \pmod{3}$: {2, 5, 8, 11, 14, 17, 20, 23, 26, ...}

$x \equiv 3 \pmod{5}$: {3, 8, 13, 18, 23, 28, ...}

$x \equiv 2 \pmod{7}$: {2, 9, 16, 23, 30, ...}

Ответ должен лежать в пересечении трёх множеств. В нашем случае наименьшим общим числом оказывается 23 (далее будут 128, 233 и т. д., то есть все решения вида $23 + 105k$).

2 способ (алгебраический)

Запишем условия как равенства с целыми параметрами:

$$x = 2 + 3q$$

$$x = 3 + 5p$$

$$x = 2 + 7t$$

Дальше последовательно «согласуем» первые два равенства, затем полученное — с третьим:

$$\begin{aligned}
2 + 3q &= 3 + 5p \\
q &= (5p + 1)/3 = p + (2p + 1)/3 \\
2p + 1 &= 3u \\
p &= (3u - 1)/2 = u + (u - 1)/2 \\
u - 1 &= 2v \\
u &= 2v + 1 \\
x = 3 + 5p &= 3 + 5(u + v) = 3 + 5(2v + 1 + v) = 8 + 15v \\
8 + 15v &= 2 + 7t \\
t &= (15v + 6)/7 = 2v + (v + 6)/7 \\
v + 6 &= 7w \\
v &= 7w - 6 \\
t &= 2(7w - 6) + w = 15w - 12 \\
x &= 2 + 7(15w - 12) = 105w - 82 = 105(w - 1) + 23
\end{aligned}$$

В результате выходит: $x = 105(w - 1) + 23$. Это значит, что наименьшее решение равно 23, а остальные получаются добавлением 105.

(Здесь подразумевается, что параметры q, p, t, u, v, w — целые числа.)

Общая формулировка и алгоритм

В теории чисел теорему формулируют на языке систем линейных сравнений.

Пусть $m_1, m_2, \dots, m_k$ — натуральные числа, попарно взаимно простые (то есть $\text{НОД}(m_i, m_j) = 1$ для любых $i \neq j$).

Пусть $r_1, r_2, \dots, r_k$ — произвольные целые числа (обычно r_i — остаток от деления на m_i). Тогда система сравнений:

$$x \equiv r_i \pmod{m_i}, i = 1, \dots, k$$

имеет решение, и все решения сравнимы по модулю $M = m_1 \cdot m_2 \cdot \dots \cdot m_k$.

Один из стандартных алгоритмов таков (известны различные доказательства):

1. Вычислить общий модуль:

$$M = m_1 \cdot m_2 \cdot \dots \cdot m_k$$

2. Вычислить частичные произведения для каждого i :

$$M_i = M/m_i$$

3. Найти обратные элементы:

для каждого i найти число y_i такое, что $M_i \cdot y_i \equiv 1 \pmod{m_i}$

(Например, используя расширенный алгоритм Евклида.)

4. Найти решение:

$$x = (r_1 \cdot M_1 \cdot y_1 + r_2 \cdot M_2 \cdot y_2 + \dots + r_k \cdot M_k \cdot y_k) \pmod{M}$$

Для нашего примера:

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{7}$$

$$M = 3 \cdot 5 \cdot 7 = 105$$

$$M_1 = 35$$

$$M_2 = 21$$

$$M_3 = 15$$

Ищем обратные:

$$M_1 \cdot y_1 \equiv 1 \pmod{3}$$

$$35 \cdot y_1 \equiv 1 \pmod{3}$$

$$y_1 = 2$$

$$M_2 \cdot y_2 \equiv 1 \pmod{5}$$

$$21 \cdot y_2 \equiv 1 \pmod{5}$$

$$y_2 = 1$$

$$M_3 \cdot y_3 \equiv 1 \pmod{7}$$

$$15 \cdot y_3 \equiv 1 \pmod{7}$$

$$y_3 = 1$$

Тогда: $x \equiv 233 \pmod{105}$, $233 = 105 \cdot 2 + 23$, значит $x \equiv 23 \pmod{105}$.

Как видите, все способы приводят к одному и тому же результату — просто разными траекториями.

 Математика с Мансур-абый