Китайская теорема об остатках

1 Постановка задачи

В общем случае дана система сравнений:

$$\begin{cases} x \underset{m_1}{\equiv} a_1 \\ x \underset{m_2}{\equiv} a_2 \\ \vdots \\ x \underset{m_n}{\equiv} a_n \end{cases}$$

Все a_i даны, нужно подобрать x, подходящий сразу под все сравнения. Например, если дана система

$$\begin{cases} x \underset{9}{\equiv} 6 \\ x \underset{10}{\equiv} 2 \\ x \underset{11}{\equiv} 9 \end{cases},$$

можно подумать, поподбирать и обнаружить, что в нее подходит число 42. Проверьте это.

Китайская теорема об остатках говорит, что, если все m_i попарно взаимно просты, т.е. НОД любых двух разных m_i и m_j равен 1, тогда система всегда имеет решение, причем все решения будут сравнимы по модулю $m_1 \cdot m_2 \cdots m_n$.

В нашем примере $(9, 10) = 1$, $(9, 11) = 1$, $(10, 11) = 1$, значит, система подходит под условие теоремы. Следовательно у нее есть решение, что мы и так знаем, потому что уже нашли 42, и следовательно все решения сравнимы по модулю $9 \cdot 10 \cdot 11 = 990$. Действительно, числа 42, $42 + 990$, $42 + 990 + 990$. $42 - 990$ и т.п. будут все подходить в систему. Убедитесь, что добавление или вычитание числа 990 не может испортить решение: дело в том, что $990 \underset{9}{\equiv} 0$, $990 \underset{10}{\equiv} 0$, $990 \underset{11}{\equiv} 0$.

2 Решение задачи

Решение задачи состоит из нескольких шагов.

2.1 Предварительные вычисления

Сначала вычислим $M = m_1 \cdot m_2 \cdots m_n$. В нашем примере $M = 990$. Потом вычислим $M_i = \frac{M}{m_i}$. Или, что тоже самое, произведение всех m кроме m_i. В нашем примере:

$$M_1 = \frac{990}{9} = 10 \cdot 11 = 110$$
$$M_2 = \frac{990}{10} = 9 \cdot 11 = 99$$
$$M_3 = \frac{990}{11} = 9 \cdot 10 = 90.$$

2.2 Решение сравнений

Необходимо решить n сравнений $M_i x_i \underset{m_i}{\equiv} a_i$. В нашем случае это:

$$110x_1 \underset{9}{\equiv} 6$$
$$99x_2 \underset{10}{\equiv} 2$$
$$90x_3 \underset{11}{\equiv} 9$$

Обратите внимание, что все сравнения надо решить независимо, и для каждого найти своё решение x_i. Давайте сделаем это. В общем случае вам может потребоваться свести сравнение к диофантовому уравнению, но здесь числа такие маленькие, что сравнения можно решить вручную. Смотрите:

Решим сравнение $\boldsymbol{110x_1 \underset{9}{\equiv} 6}$

Заменим 110 по модулю 9: $110 \underset{9}{\equiv} 2$:

$$2x_1 \underset{9}{\equiv} 6$$

Сократим на 2:

$$x_1 \underset{9}{\equiv} 3.$$

Решим сравнение $\boldsymbol{99x_1 \underset{10}{\equiv} 2}$

Заменим 99 по модулю 10: $99 \underset{10}{\equiv} -1$:

$$-x_2 \underset{10}{\equiv} 2$$

Домножим на -1:

$$x_2 \underset{10}{\equiv} -2.$$

Решим сравнение $\boldsymbol{90x_1 \underset{11}{\equiv} 9}$

Заменим 90 по модулю 11: $90 \underset{11}{\equiv} 2$:

$$2x_3 \underset{11}{\equiv} 9 \underset{11}{\equiv} -2$$

Сократим на 2:

$$x_3 \underset{11}{\equiv} -1.$$

2.3 Выписываем ответ

Ответ вычисляется по формуле

$$x \underset{M}{\equiv} M_1 x_1 + M_2 x_2 + \cdots + M_n x_n$$

в нашем примере это

$$x \underset{990}{\equiv} 110 \cdot 3 + 99 \cdot (-2) + 90 \cdot (-1) = 42$$