ЛЕКЦИЯ 9

КИТАЙСКАЯ ТЕОРЕМА ОБ ОСТАТКАХ

Одним из важных результатов теории чисел является так называемая китайская теорема об остатках (КТО). По существу эта теорема утверждает, что можно восстановить целое число по множеству его остатков от деления на числа из некоторого набора попарно взаимно простых чисел. Эта теорема была доказана приблизительно в 100 году до н.э. Существуют несколько формулировок китайской теоремы об остатках. Представим здесь некоторые из них. Обозначим через Z_n кольцо вычетов по модулю n.

Теорема. Если $n = n_1 n_2 \ldots n_k$, где n_i, $1 \le I \le k$, – взаимно простые числа, то кольцо Z_n является прямой суммой колец Z_{ni}.

Теорема. Пусть n_i, $1 \le i \le k$, взаимно простые числа и пусть a_i целые числа. Тогда существует такое число x, что имеет место

$$\begin{gathered} x \equiv a_1 \bmod n_1, \\ x \equiv a_2 \bmod n_2, \\ \ldots \\ x \equiv a_k \bmod n_k . \end{gathered}$$

Теорема. Пусть модули системы линейных сравнений являются взаимно простыми. Это означает, что общий делитель двух чисел n_i и n_j равен единице, т. е. $(n_i, n_j) = 1$ при $1 \le i, j \le k$. В этом случае существует класс вычетов Z_{ni}, который удовлетворяет условию

$$Z_{ni} \equiv 0 \bmod n_j.$$

Наконец, рассмотрим еще одну формулировку теоремы, которую будем использовать в практических работах.

Теорема. Пусть m_i, $1 \le I \le k$, – взаимно простые числа и

$$M = m_1 m_2 \ldots m_k.$$

Пусть

$$a_i,\ 0 \le a_i \le m_i,$$

целые числа. Введем обозначение $M_i = M/m_i$. Пусть N_i число, которое удовлетворяет сравнению

$$M_i N_i \equiv 1\ mod\ m_i.$$

При этих условиях сравнение

$$x \equiv a_i \text{ mod } m_i$$

имеет на интервале [0, M – 1] единственное решение, которое определяется формулой

$$x = a_1 N_1 M_1 + a_2 N_2 M_2 + \ldots + a_k N_k M_k.$$

В рамках условий теоремы китайская теорема об остатках утверждает, что существует взаимно однозначное соответствие между целыми числами и некоторым наборами целых чисел. Другими словами, для каждого целого числа B найдется соответствующий ему единственный набор чисел

$$b_1, b_2, \ldots, b_k,$$

и наоборот, для каждого набора чисел (b_1, b_2, …, b_k) найдется единственное соответствующему этому набору число B.

Пример. Решить систему сравнений

$$x \equiv a_1 \text{ mod } 4,$$
$$x \equiv a_2 \text{ mod } 5,$$
$$x \equiv a_3 \text{ mod } 7,$$

где $m_1 = 4$, $m_2 = 5$, $m_3 = 7$. Определим число

$$M = m_1 m_2 m_3 = 4 \times 5 \times 7 = 140.$$

Вычислим

$$M_1 = M/m_1 = 140/4 = 35,$$
$$M_2 = M/m_2 = 140/5 = 28,$$
$$M_3 = M/m_3 = 140/7 = 20.$$

Вычислим N_1, N_2, и N_3 из следующих сравнений:

$$N_1 M_1 = 35N_1 \equiv 1 \bmod 4,$$
$$N_2 M_2 = 28N_2 \equiv 1 \bmod 5,$$
$$N_3 M_3 = 20N_3 \equiv 1 \bmod 7.$$

Решаем первое сравнение

$$35N_1 \equiv 1 \bmod 4.$$

Определяем функцию Эйлера

$$\varphi\,(4) = \varphi\,(2^2) = 2^{2\,-\,1}(2 - 1) = 2.$$

Тогда из теоремы Ферма следует:

$$N_1 = 35^{\varphi\,(4)\,-\,1} \bmod 4 = 35^{2-1} \bmod 4 = 35 \bmod 4 = 3.$$

Проверка решения 1первого сравнения $35N_1 \equiv 1 \bmod 4$.
Подставляем значение $N_1 = 3$ в сравнение

$$35N_1 \equiv 1 \bmod 4,$$

получаем

$$35 \times 3 \bmod 4 \equiv 105 \bmod 4 \equiv 1 \bmod 4.$$

Решаем 2второе сравнение

$$28N_2 \equiv 1 \bmod 5.$$

Определяем функцию Эйлера $\varphi(5) = 5 - 1 = 4$. Тогда из теоремы Ферма следует

$$N_2 = 28^{\varphi(5) - 1} \bmod 5 = 28^{4 - 1} \bmod 4 =$$
$$=28^3 \bmod 5 = 112 \bmod 5 = 2 \bmod 5.$$

Проверка решения второго сравнения $28N_2 \equiv 1 \bmod 5$. Подставляем значение $N_2 = 2$ в сравнение

$$28N_2 \equiv 1 \bmod 5,$$

получаем

$$28 \times 2 \bmod 5 \equiv 56 \bmod 5 \equiv 1 \bmod 5.$$

Решаем третье сравнение

$$20N_3 \equiv 1 \bmod 7.$$

Определяем функцию Эйлера φ(7)=7 – 1=6. Тогда из теоремы Ферма следует

$$N_3 = 20^{\varphi(7) - 1} \bmod 7 = 20^{6- 1} \bmod 7 =$$
$$= 20^5 \bmod 7 = 20 \bmod 7 = 6 \bmod 7 .$$

Проверка решения третьего сравнения $20N_3 \equiv 1 \bmod 7$. Подставляем значение $N_3 = 6$ в сравнение

$$20N_2 \equiv 1 \bmod 7,$$

имеем

$$20 \times 6 \bmod 7 \equiv 120 \bmod 7 \equiv 1 \bmod 7.$$

Окончательно получаем, что решение системы сравнений

$$x \equiv a_1 \bmod 4,$$
$$x \equiv a_2 \bmod 5,$$
$$x \equiv a_3 \bmod 7,$$

определяется формулой

$$x = (a_1N_1M_1 + a_2N_2M_2 + a_3N_3M_3 =$$
$$= (35 \times 3a_1 + 28 \times 2a_2 + 20 \times 6a_3) \bmod 140.$$