Китайская теорема об остатках для двух элементов

Пусть m, n - два взаимно простых целых числа. Тогда для любой пары (a, b) целых чисел существует целое число c такое, что

$$\begin{cases} x \equiv a (\mathrm{mod}\ m), \\ x \equiv b (\mathrm{mod}\ n) \end{cases}$$

тогда и только тогда, когда $x \equiv c (\mathrm{mod}\ m \cdot n)$

если c^1 другое решение этой системы, то

$$c \equiv c^1 (\mathrm{mod}\ m \cdot n).$$

Пример:

Рассмотрим два простых числа n=31, m=17. Соответствующие им коэффициенты Безу u= -6, v=11, т.е.

$$-6 \cdot 31 + 11 \cdot 17 = 1$$

Произведение n на m равно 527. Для данных y и z система

$$\begin{cases} x \equiv y (\mathrm{mod}\, 31) \\ x \equiv z (\mathrm{mod}\, 17) \end{cases}$$

имеет решение $11 \cdot 17 \cdot y + 31 \cdot (-6) \cdot z$.

Вычислительные формулы.

Вычисление

$x = n \cdot (u \cdot (b - a) \bmod m) + a,$

дает единственное целое число из интервала $[0, n \cdot m)$, удовлетворяющее сравнениям

$$\begin{cases} x \equiv a (\bmod\ n), \\ x \equiv b (\bmod\ m). \end{cases}$$

Пример:

Исходные данные: n = 31, m = 17, u =-6, y = 24, z = 9. Сначала подсчитаем $u(z - y) \bmod m$ = -6· (9 – 24) mod 17 = -12, умножаем это на n и прибавляем y. Получаем x = 31·(-12) + 24 = 179, что и является решением.

Китайская теорема об остатках для **r** элементов

Пусть $n_1, n_2, \ldots, n_r$ - попарно взаимно простые числа. Пусть $a_1, a_2, \ldots, a_r$ произвольно целые числа. Тогда система

$$\begin{cases} x \equiv a_1 (\mathrm{mod}\, n_1); \\ x \equiv a_2 (\mathrm{mod}\, n_2); \\ \ldots\ldots\ldots\ldots\ldots; \\ x \equiv a_r (\mathrm{mod}\, n_r); \end{cases}$$

имеет по крайней мере одно решение. Кроме того, если x' – другое решение этой системы, то

$$x \equiv x' (\mathrm{mod}\ n_1 \cdot n_2 \cdot \ldots \cdot n_r).$$

Вычислительные формулы.

Пусть $n_1, n_2, \ldots, n_r$ - попарно взаимно простые числа. Тогда решения системы сравнений $x \equiv x_i \pmod{n_i}$. находятся из последовательности вычислений:

$$\begin{cases} y_1 = x_1 \bmod n_1, \\ y_2 = N_2(C_2(x_2 - y_1) \bmod n_2) + y_1, \\ y_3 = N_3(C_3(x_3 - y_2) \bmod n_3) + y_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ y_r = N_r(C_r(x_r - y_{r-1}) \bmod n_r) + y_{r-1}, \end{cases}$$

в которой $N_i = \prod_{j<i} n_j$ коэффициент C_i удовлетворяет

условиям $C_i N_i \equiv 1 \pmod{n_i}$ и получены при помощи алгоритма Евклида для N_i и n_i. При этих условиях число y_r будет единственным решением системы сравнений на интервале $[0, n_1 \cdot n_2 \cdot \ldots \cdot n_r)$