

## Франц Герман

### Алгоритм нахождения перестановок

[franz.h-n@yandex.ru](mailto:franz.h-n@yandex.ru)

В некоторых задачах, решаемых на компьютере, возникает необходимость нахождения перестановок из  $n$  элементов.

Для небольших  $n$  это можно сделать простым перебором, но с увеличением  $n$ , нахождение всех перестановок перебором становится занятием очень трудоёмким. В таком случае удобно применять следующий алгоритм.

В данной заметке мы покажем один из способов алгоритмизации данной задачи.

Докажем теорему, применение которой понадобится в дальнейшем для построения нашего алгоритма.

#### Теорема:

Если даны два числа  $X$  и  $Y$   $p$ -ичной системы счисления с одинаковой суммой поразрядных цифр, то справедливо равенство:

$$X \equiv Y \pmod{p-1} \quad (1)$$

**Пример:**  $X = 147_{10}$ ,  $Y = 2532_{10}$ , где индекс внизу числа указывает на основание системы счисления. В данном случае  $p = 10$  (в дальнейшем для десятичной, привычной нам, системы счисления индекс будем опускать).

Действительно, для  $X$  имеем:  $1+4+7=12$ . Для  $Y$ :  $2+5+3+2=12$ , и  $2532-147=2385$ . Число  $2385:9$ , т. е. эта запись говорит, что число  $2385$  делится на  $9$  без остатка, что удовлетворяет нашей теореме.

Ещё **пример:**  $X = 214_5$ ,  $Y = 403_5$ . Проверим, выполняется ли условие теоремы:  $2+1+4 = 4+0+3$ . Далее, для удобства вычислений переведём данные числа в привычную нам систему счисления (десятичную).

$$214_5 = 2 \cdot 5^2 + 1 \cdot 5^1 + 4 \cdot 5^0 = 59$$

$$403_5 = 4 \cdot 5^2 + 0 \cdot 5^1 + 3 \cdot 5^0 = 103$$

Проверим справедливость теоремы:  $103-59 = 44$ ,  $44:4$ , помним, что  $p = 5$ .

Теперь приступим к доказательству теоремы.

#### Доказательство:

Пусть имеем два числа  $X$  и  $Y$   $p$ -ичной системы счисления. Запишем наши числа в развёрнутом виде:

$$X = \overline{x_n x_{n-1} \dots x_1 x_0} = x_n \cdot p^n + x_{n-1} \cdot p^{n-1} + \dots + x_1 \cdot p^1 + x_0 \cdot p^0$$

$$Y = \overline{y_m y_{m-1} \dots y_1 y_0} = y_m \cdot p^m + y_{m-1} \cdot p^{m-1} + \dots + y_1 \cdot p^1 + y_0 \cdot p^0$$

Обозначим через  $S(x)$  и  $S(y)$  поразрядные суммы цифр чисел  $X$  и  $Y$  соответственно, т. е.  $S(x) = x_n + x_{n-1} + \dots + x_1 + x_0$  и  $S(y) = y_m + y_{m-1} + \dots + y_1 + y_0$ , где  $S(x) = S(y)$ .

Докажем, что  $p^k \equiv 1 \pmod{p-1}$  или, что тоже самое  $\frac{p^k - 1}{p-1} = n$  - целое число.

Рассмотрим конечную геометрическую прогрессию, знаменатель которой целое число  $p$ :  $1, p, p^2, \dots, p^{k-2}, p^{k-1}$ . Сумма членов этой прогрессии вычисляется по формуле:  $\sum_{x=0}^{k-1} p^x = \frac{p^{k-1} \cdot p - 1}{p-1} = \frac{p^k - 1}{p-1}$ . А т. к.  $p$ - целое число, то и сумма будет целым числом. Т. е. справедливость выражения  $p^k \equiv 1 \pmod{p-1}$  доказана.

Используя правила алгебры сравнений можем записать.

$$x_n p^n \equiv x_n \pmod{p-1},$$

$$x_{n-1} p^{n-1} \equiv x_{n-1} \pmod{p-1},$$

и т. д.

$$x_0 p^0 \equiv x_0 \pmod{p-1}$$

И также, пользуясь правилами алгебры сравнений, получаем:

$$x_n \cdot p^n + x_{n-1} \cdot p^{n-1} + \dots + x_1 \cdot p^1 + x_0 \cdot p^0 \equiv (x_n + x_{n-1} + \dots + x_1 + x_0) \pmod{p-1}$$

или  $X \equiv S(x) \pmod{p-1}$ .

Аналогично доказываем, что и  $Y \equiv S(y) \pmod{p-1}$ , а т. к.  $S(x) = S(y)$ , то можем записать:  $X - Y \equiv 0 \pmod{p-1}$  или  $X \equiv Y \pmod{p-1}$ .

Что и требовалось доказать.

Пусть нам требуется найти все перестановки из  $k$  элементов.

Рассмотрим две такие перестановки:

$$P_1 = (k-1, k-2, \dots, 1, 0) \text{ и } P_2 = (0, 1, 2, \dots, k-1).$$

Сопоставим каждой перестановке число  $k$ -ичной системы счисления  $N_1$  и  $N_2$  соответственно:

$N_1 = \overline{x_{k-1} \dots x_1 x_0}_k$  и  $N_2 = \overline{x_0 x_1 \dots x_{k-1}}_k$ , где нижний индекс за выражением числа, как мы и договаривались, указывает на систему счисления, в которой оно записано. В данном случае мы рассматриваем числа в  $k$ -ичной системе счисления. А формула соответствия цифр числа и элементов перестановки имеет вид:  $x_i = i$ .

Переведём числа  $N_1$  и  $N_2$  в десятичную систему счисления:

$$N_1 = x_{k-1} \cdot (k)^{k-1} + x_{k-2} \cdot (k)^{k-2} + \dots + x_1 \cdot (k)^1 + x_0 \cdot (k)^0,$$

$$N_2 = x_0 \cdot (k)^{k-1} + x_1 \cdot (k)^{k-2} + \dots + x_{k-2} \cdot (k)^1 + x_{k-1} \cdot (k)^0.$$

Теперь покажем алгоритм для нахождения перестановок в пошаговой записи понятной компьютеру:

1.  $N_1$  соответствует перестановке  $P_1$
2.  $N_1 = N_1 - (k - 1)$
3. Если  $N_1 = N_2$ , то  $N_2$  соответствует последней перестановке  $P_2$ . И на этом работа алгоритма заканчивается.
4. Если  $N_1 \neq N_2$ , то новое число  $N_1$  переводим в  $k$ -ичную систему счисления и смотрим, все ли цифры в этом числе различные. Если да, то новое число  $N_1$  соответствует новой перестановке. Переходим к пункту 2.

Пункт 2. мог бы выглядеть иначе:  $N_1 = N_1 - 1$ , но вышедоказанная теорема позволяет задать именно  $N_1 = N_1 - (k - 1)$ , т. к. числа, соответствующие перестановкам, имеют одну и ту же поразрядную сумму цифр.

**Пример:** найдём все перестановки из трёх элементов. Известно, что таких перестановок должно быть  $3! = 6$ . Покажем работу алгоритма в развёрнутом виде.

$$P_1 = (210), P_6 = (012)$$

$$N_1 = 2 \cdot 3^2 + 1 \cdot 3^1 + 0 \cdot 3^0 = 21, \quad N_6 = 0 \cdot 3^2 + 1 \cdot 3^1 + 2 \cdot 3^0 = 5$$

$$N_2 = N_1 - (k - 1) = 21 - 2 = 19 = 201_3, \quad N_2 \neq N_6, \text{ следовательно } P_2 = (201)$$

$$N_3 = N_2 - (k - 1) = 19 - 2 = 17 = 122_3, \quad \text{не подходит (см. пункт 4. алгоритма)}$$

$$N_3 = N_3 - (k - 1) = 17 - 2 = 15 = 120_3, \quad N_3 \neq N_6, \text{ следовательно } P_3 = (120)$$

$$N_4 = N_3 - (k - 1) = 15 - 2 = 13 = 111_3, \quad \text{не подходит}$$

$$N_4 = N_4 - (k - 1) = 13 - 2 = 11 = 102_3, \quad N_4 \neq N_6, \text{ следовательно } P_4 = (102)$$

$$N_5 = N_4 - (k - 1) = 11 - 2 = 9 = 100_3, \quad \text{не подходит}$$

$$N_5 = N_5 - (k - 1) = 9 - 2 = 7 = 021_3, \quad N_5 \neq N_6, \text{ следовательно } P_5 = (021)$$

$N_6 = N_5 - (k - 1) = 7 - 2 = 5 = 012_3$ , последняя перестановка. Т. о. все перестановки найдены.