Разбор задачи «G. Шестеренки»

Автор задачи и разбора — Иван Богатый

Решение на 30 баллов

Для получения 30 баллов досточно было запрограммировать перебор всех троек, которые можно получить из первой, и проверить, есть ли среди них вторая. Для этого нужно моделировать один поворот шестеренок до тех пор, пока мы не встретим или ту тройку, с которой начинали (и тогда ответ `NO`), или ту, которую хотим получить (и тогда ответ `YES`).

Решение на 60 баллов

Пусть x — количество поворотов, которое необходимо сделать, чтобы перейти от первой конфигурации ко второй, если это возможно. Из условия задачи, мы имеем следующие три соотношения на x:

$$\begin{cases} x \equiv a_1 - b_1 \mod n, \\ x \equiv b_2 - a_2 \mod m, \\ x \equiv a_3 - b_3 \mod k. \end{cases} \qquad (1)$$

Чтобы ответить на вопрос задачи, надо всего лишь узнать, имеет ли данная система решение. Для этого необходимо и достаточно проверить ее по модулю каждого простого делителя n,m,k. Более точно, если $n = n' \cdot p^{e_1}, m = m' \cdot p^{e_2}, k = k' \cdot p^{e_3}$, и e_1, e_2, e_3 максимальны, то должно выполняться

$$\begin{cases} x \equiv a_1 - b_1 \mod p^{e_1}, \\ x \equiv b_2 - a_2 \mod p^{e_2}, \\ x \equiv a_3 - b_3 \mod p^{e_3} \end{cases} \qquad (2)$$

для всех простых p.

Проверить совместность (существование решения) такой системы нетрудно: x определяется из сравнения, в котором e_i максимально. Полученное значение надо подставить в два других сравнения, и убедиться, что не возникло противоречий.

Если, например, $e_1 \geq e_2$ и $e_1 \geq e_3$, то совместность системы (2) равновильна выполнению равенств $a_1 - b_1 \equiv b_2 - a_2 \mod p^{e_2}$ и $a_1 - b_1 \equiv a_3 - b_3 \mod p^{e_3}$.

По китайской теореме об остатках, начальная система (1) имеет решение тогда и только тогда, когда для всех простых p системы (2) совместны. Естественно, имеет смысл проверять лишь те p, которые являются делителями хотя бы одного из n, m, k. Таким образом, мы получаем алгоритм, работающий за время разложения n, m, k на простые, т.е. укладывающийся в ограничения $n, m, k \leq 10^9$.

Примечание. Рассмотрим произвольную систему из двух сравнений

$$\begin{cases} x \equiv a \mod n, \\ x \equiv b \mod m. \end{cases} \qquad (3)$$

Обозначим $g = \gcd(n, m)$ (наибольший общий делитель). Тогда система (3) равносильна следующей:

$$\begin{cases} x \equiv a \mod g, \\ x \equiv a \mod n/g, \\ x \equiv b \mod g, \\ x \equiv b \mod m/g, \end{cases} \tag{4}$$

а она совместна тогда и только тогда, когда $a \equiv b \mod g$.

Используя описанный механизм, исходную систему (1) можно свести к системе из, вообще говоря, девяти сравнений с попарно взаимно простыми модулями (существование решения которой гарантирует китайская теорема об остатках), либо обнаружить ее несовместность. Так можно было решить задачу на 100 баллов, однако здесь мы рассмотрим другой подход, дающий более простой способ решения исходной задачи.

Правильное решение

Докажем, что две тройки (a_1, a_2, a_3) и (b_1, b_2, b_3) принадлежат одной последовательности поворотов тогда и только тогда, когда удовлетворяют системе сравнений

$$\begin{cases} a_2 + a_1 \equiv b_2 + b_1 \mod \gcd(m, n), \\ a_2 + a_3 \equiv b_2 + b_3 \mod \gcd(m, k), \\ a_1 - a_3 \equiv b_1 - b_3 \mod \gcd(n, k). \end{cases} \tag{5}$$

Или, эквивалентно:

$$\begin{cases} a_2 + a_1 \equiv b_2 + b_1 \mod \gcd(m, n), \\ a_2 + a_3 \equiv b_2 + b_3 \mod \gcd(m, k), \\ a_1 - a_3 \equiv b_1 - b_3 \mod \gcd(n, k)/\gcd(n, m, k). \end{cases}$$

При этом мы неявно получим еще один способ решения с помощью расширенного алгоритма Евклида.

Необходимость. При одном повороте на первой шестеренке вместо числа a_1 возникает число $a_1 - 1$ или $a_1 - 1 + n$, на второй шестеренке вместо числа a_2 возникает число $a_2 + 1$ или $a_2 + 1 - m$, на третьей шестеренке вместо числа a_3 возникает число $a_3 - 1$ или $a_3 - 1 + k$. Видно, что при одном повороте, а значит и при любом их количестве, величины

$$a_2 + a_1 \mod \gcd(m, n), \quad a_2 + a_3 \mod \gcd(m, k), \quad a_1 - a_3 \mod \gcd(n, k)$$

не меняются.

Достаточность.

Назовем *канонической* любую тройку вида $(1, \tilde{a}_2, \tilde{a}_3)$, где $1 \le \tilde{a}_2 \le \gcd(n, m)$ и $1 \le \tilde{a}_3 \le \gcd(\operatorname{lcm}(n, m), k)$ (lcm — наименьшее общее кратное).

Докажем, что сделав правильно подобранное число поворотов, конфигурацию (a_1, a_2, a_3) можно перевести в некоторую каноническую $(1, \tilde{a}_2, \tilde{a}_3)$. Сделав сперва $a_1 - 1$ поворотов, мы придем к эквивалентной тройке $(1, \bar{a}_2, \bar{a}_3)$. По алгоритму Евклида существуют такие целые числа x и y, что $\gcd(n, m) = ym - xn$. Тогда после совершения xn поворотов число на первой шестеренке не изменится, а число на второй шестеренке уменьшится ровно на $\gcd(n, m)$. Опять же, по алгоритму Евклида существуют такие целые числа z и t, что $\gcd(\operatorname{lcm}(n, m), k) = z \operatorname{lcm}(n, m) - tk$. Тогда после совершения $z \operatorname{lcm}(n, m) n$ поворотов числа на первой и второй шестеренках не изменятся, а число на третьей уменьшится ровно на $\gcd(\mathrm{lcm}(n, m), k)$. Таким образом, мы можем «подкрутить» конфигурацию $(1, \bar{a}_2, \bar{a}_3)$ так, чтобы получить из нее каноническую.

Полученная тройка $(1, \tilde{a}_2, \tilde{a}_3)$ эквивалентна первоначальной тройке, поэтому связана с ней сравнениями (5). Докажем, что система (5) определяет ее однозначно. Действительно, пусть еще одна каноническая тройка $(1, \hat{a}_2, \hat{a}_3)$ удовлетворяет системе сравнений (5). Тогда

$$\begin{cases} \tilde{a}_2 \equiv \hat{a}_2 \mod \gcd(m, n), \\ \tilde{a}_2 + \tilde{a}_3 \equiv \hat{a}_2 + \hat{a}_3 \mod \gcd(m, k), \\ \tilde{a}_3 \equiv \hat{a}_3 \mod \gcd(n, k). \end{cases}$$

Из первого сравнения и ограничений на числа $\tilde{a}_2$ и $\hat{a}_2$ вытекает равенство $\tilde{a}_2 = \hat{a}_2$. Поэтому два последних равенства из системы сравнений принимают вид

$$\begin{cases} \tilde{a}_3 \equiv \hat{a}_3 \mod \gcd(m, k), \\ \tilde{a}_3 \equiv \hat{a}_3 \mod \gcd(n, k), \end{cases}$$

что эквивалентно одному сравнению

$$\tilde{a}_3 \equiv \hat{a}_3 \mod \mathrm{lcm}(\gcd(m, k), \gcd(n, k)).$$

А так как $\mathrm{lcm}(\gcd(m, k), \gcd(n, k)) = \gcd(\mathrm{lcm}(n, m), k)$, то $\tilde{a}_3 = \hat{a}_3$.

Итак, мы показали, что для любой тройки (a_1, a_2, a_3) существует единственная эквивалентная ей каноническая тройка. Поэтому конфигурации (a_1, a_2, a_3) и (b_1, b_2, b_3) принадлежат одной последовательности тогда и только тогда, когда эквивалентные им канонические тройки совпадают, что равносильно выполению для них системы (5). Остается воспользоваться предположением о том, что система (5) выполнена для исходных конфигураций.