Самым важным и тонким местом алгоритма является количество цепочек — $\gcd(s,n)$, обозначим его $d \stackrel{\text{def}}{=} \gcd(s,n)$. Нужно доказать, что любая позиция $q \in \overline{0, n-1}$ (где n — длина массива) (I) попадает хотя бы в одну цепочку и (II) что эта цепочка единственна.

(I) можно сформулировать так:

$$\exists i \in \overline{0, d-1}, \exists r_1, r_2 \in \mathbb{Z} : q = i + sr_1 - nr_2.$$

Здесь i это индекс цепочки (по совместительству номер элемента массива, в котором она начинается).

Определение. Два числа $a, b \in \mathbb{Z}$ называются сравнимыми по модулю $m \in \mathbb{Z}_+$ и пишут

$$a \equiv b \pmod{m} \tag{1}$$

если

$$\exists r \in \mathbb{Z} : \ a - b = rm.$$

Выражение (**??**) называют *сравнением по модулю m*.

В свете этого определения (I) можно записать так:

$$\exists i \in \overline{0, d-1} \ \exists r \in \mathbb{Z} : sr \equiv q - i \pmod{n} \tag{2}$$

Теорема. Для данных $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}_+$ сравнение

$$ax \equiv b \pmod{m}$$

разрешимо для некоторого x тогда и только тогда, когда $\gcd(a,m)|b$. («$|$» означает «делит», то есть, в данном случае: «b кратно $\gcd(a,m)$».)

Очевидно, в (2) можно выбрать i такой, чтобы $d|q-i$ (i должен равняться остатку от деления q на d), таким образом, это сравнение рарешимо для некоторого r и (I) доказано.

Рассмотрим вопрос (II) единственности. Покажем сначала, что никакая цепочка не выскакивает на начало другой цепочки, то есть не попадает в первые d лементов массива кроме как в своё собственное начало. Предположим обратное: для некоторых $r_1, r_2 \in \mathbb{Z}$ выполнено $i + sr_1 - nr_2 = q$, где $i \in \overline{0, d-1}$, $q \in \overline{0, d-1}$ и $i \neq q$ (иначе это случай попадания в своё начало). Так как $d|sr_1, nr_2$, то необходимо $d|q-i$, однако $q - i \in \overline{1-d, d-1} \setminus \{0\}$ — противоречие.

Очевидно, если одна цепочка выскакивает на k-ое по счету звено другой, то k шагов назад она необходимо попадала бы на начало этой другой цепочки, что невозможно по доказанному выше. Таким образом, (II) доказано и вместе с этим завершено обоснование алгоритма.