1 Условие

Научитесь генерировать большие числа Кармайкла с тремя большими простыми делителями.

2 Решение

2.1 Обозначения

- $\mathcal{C}$ — множество всех чисел Кармайкла.
- $\mathcal{P}$ — множество всех простых чисел.

2.2 Теория

Теорема 1.

- $\forall i \;\; p_i \in \mathcal{P}$
- $n = \prod_i p_i$
- $\forall i \;\; p_i - 1 \equiv 0 \mod n - 1$

Тогда $n \in \mathcal{C}$. В обратную сторону также верно.

Доказательство. $\lhd a : gcd(a, n) = 1$.

По теореме Ферма:

$$\begin{aligned} a^{p_i - 1} &\equiv 1 \mod p_j \\ p_i - 1 &\equiv 0 \mod n - 1 \\ a^{n-1} &\equiv 1 \mod p_j \\ a^{n-1} &\equiv 1 \mod n \end{aligned}$$

□

Теорема 2.

- $p \in \mathcal{P}$
- $n = pu$

Тогда $p - 1 \equiv 0 \mod n - 1 \Leftrightarrow p - 1 \equiv 0 \mod u - 1$.

Доказательство.

$$(n - 1) - (u - 1) = n - u = pu - u = (p - 1)u$$

Если $p - 1$ делит ровно одно из $\{n - 1, u - 1\}$, то левая часть не делится на $p - 1$, а правая делится — противоречие. □

2.3 Первый метод

Будем искать $n \in \mathcal{C} : n = p \cdot q \cdot r, p < q < r$.
По теореме 1:

$$\begin{cases} p - 1 \equiv 0 \mod n - 1 \\ q - 1 \equiv 0 \mod n - 1 \\ r - 1 \equiv 0 \mod n - 1 \end{cases}$$

По теореме 2:

$$\begin{cases} p - 1 \equiv 0 \mod qr - 1 \\ q - 1 \equiv 0 \mod pr - 1 \\ r - 1 \equiv 0 \mod pq - 1 \end{cases} \tag{1}$$

Если зафиксировать p, q, то можно перебрать все $d \equiv 0 \mod pq - 1$, такие что $q < d$. Для каждого d нужно проверить, что $d + 1 \in \mathcal{P}$. Если это так, третье условие выполнено.

Рис. 1: Кот, который мотивировал меня заниматься этой страшной задачей.

2.4 Второй метод

Для $p = 6N + 1, q = 12N + 1, r = 18N + 1$ условие (1) выполнено:

$$\begin{cases} 6N \equiv 0 \mod 216N^2 + 30N \\ 12N \equiv 0 \mod 108N^2 + 24N \\ 18N \equiv 0 \mod 72N^2 + 18N \end{cases}$$

и нужно только проверять на простоту. Небольшой трюк: если для $\tilde{N}$ p не простое, то $2\tilde{N}$ и $3\tilde{N}$ рассматривать не нужно.

3 Анализ

3.1 Первый метод

Генерировать все $p, q < n : p, q \in \mathcal{P}$ занимает $\mathcal{O}(n / \log\log n)$ и асимптотически мы найдём $\frac{n^2}{\log^2 n}$ пар, т.е.

$$\frac{\log^2 n}{n^2} \cdot \frac{n}{\log\log n} = \frac{\log^2 n}{n \log\log n}$$

итераций на пару. Я не придумал, как оценить число делителей $pq - 1$, поэтому дальше не анализируется.

3.2 Второй метод

Проверить на простоту детерминированно занимает $\mathcal{O}(\log^6 n)$ с помощью AKS. Т.к. вероятность случайно выбрать простое число есть $\Theta\left(\frac{1}{\log n}\right)$, то вероятность выбрать 3 простых числа — $\Theta\left(\frac{1}{\log^3 n}\right)$. Таким образом, получается $3 \cdot \mathcal{O}(\log^6 n) \cdot \Theta(\log^3 n) = \mathcal{O}(\log^9 n)$.

Ещё можно использовать модификацию AKS за $\mathcal{O}(\log^3 n)$, которая работает, если гипотеза Агравала верна, и если мы выдадим неверный ответ, то заявляем всем, что мы её опровергли :).