Студент: Александр Никулин
Дата: 14 декабря 2020 г.

Задача 1. *Малая теорема Ферма говорит, что* $a^{p-1} \equiv 1 \bmod p$ *(*p *простое).*
Обозначим $ord(a) = \min x > 0 \colon a^x \equiv 1 \bmod p$. $g \colon$ $ord(g) = p-1$ *называют первообразным корнем Даны простое* p *и* z *(*$0 < z < p$*).*

(a) *Подумайте, каким может быть* (z)*?*
(b) *За сколько максимально быстро вы можете проверить, является ли* z *первообразным корнем?*

Решение.

(a) (z) можно оценить сверху как $p-1$, т.к. по теореме Ферма определение будет выполнено, однако может найтись и меньший x. Докажем, что если такой найдется, то он будет одним из делителей $p-1$. От противного, пусть $k = \text{ord}(z)$ не является делителем, тогда можно записать $p-1 = k*q+r, 0 \le r < k$. Тогда $z^{p-1} = z^{kq}z^r = 1^q z^r = z^r$. Получили, что $1 \equiv z^{p-1} = z^r$, но $r < k$, а значит мы нашли меньший такой подходящий x, чем k - противоречие. Отсюда следует, что $r = 0$, то есть $\text{ord}(z) | p-1$.
(b) Можно перебрать все делители числа $p-1$, тогда за $\mathcal{O}(\sqrt{p-1})$ т.к. нужно факторизовать. Можно быстрее, если доказать, что достаточно проверить только делители вида $\frac{p-1}{p_i}$, где p_i - простой делитель. По традиции, есть поистине чудесное доказательство этого факта, но сюда оно уже не влезет, да и количество операций тогда оценить сложнее.

Задача 2.

Решение.

Задача 3. *Обозначим* i*-е по возрастанию простое число, как* p_i*. Назовём число* b*-гладким, если все его простые делители не превосходят* p_b*. Дано* $n \le 10^6$*. Для каждого* $b \le n$ *найдите количество* b*-гладких чисел от* 1 *до* n*.*

Решение. Мы уже умеем делать Решето Эратосфена за $\mathcal{O}(n \log\log n)$, попробуем применить его здесь. Минимальную b-гладкость можно определить по максимальному простому числу в разложении числа на простые множители. Например, число $6 = 2*3$ является 2-гладким, 3-гладким и т.д. (по определению), но не 1-гладким. Видно, что в количество n-гладких чисел вложено количество всех меньших. Поэтому, для каждого b, надо найти количество чисел в разложении которых на простые числа b будет максимальным, а также числа в разложении которых все простые меньше b. То есть числа вида $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, где $p_i \le b$, а произведение $\le n$.

Во время прохода алгоритма Эратосфена будем для каждого числа хранить максимальное простое число, для которого это число было вычеркнуто. В конце у нас будет массив числе длины n, тогда достаточно для каждого уникального посчитать частоту, после чего посчитать префиксные суммы (сколько чисел у которых максимальное 2, + сколько чисел у которых максимальное 3 и т.д.). Тогда за два прохода посчитаем, что нужно.

Асимптотика: $\mathcal{O}(2n + n \log\log n) = \mathcal{O}(n \log\log n)$

Задача 4. *Известны открытый ключ* $(n, 3)$ *и закрытый ключ* (n, d) *системы RSA. Известно, что* n *— произведение двух разных простых. Разложите* n *на множители.* $\mathcal{O}(poly(\log n))$*.*

Решение. Нужно найти p и q. Мы знаем (из системы RSA), что $3d \equiv 1 \mod \phi(n)$, то есть по мультипликативности функции Эйлера $3d \equiv 1 \mod (p-1)(q-1) \Rightarrow 3d = k(p-1)(q-1)+1$, откуда $k \in \{1, 2\}$ т.к $d < (p-1)(q-1)$. Тогда, по обратной теореме Виета (если выразить из предыдущего $p+q$, а $pq = n$) p и q находятся из квадратных уравнений: $x^2 - (n - 3d + 2)x + n = 0$ при $k = 1$; $x^2 + (\frac{2n-3d+3}{2})x + n = 0$ при $k = 2$. Так как мы договорились работать с короткими числами, то это просто фиксированное количество операций, поэтому асимптотика $\mathcal{O}(1)$.