Студент: Маргарита Чудова
Группа: 2
Дата: 27 апреля 2022 г.

---

1. Докажем по индукции: предположим, что до i-ого элемента все элементы являются делителями. База очевидна для 1. Хотим проверить:

   ```
   i*f[i] % p = 1
   ```

   Заметим, что:

   ```
   i*f[i] = (p - f[p%i])* i *(p // i) % p = (p - f[p%i])*(p - p % i) % p
   ```

   Раскроем скобки — только `f[p % i]*(p % i)` не будет включать множителя p. Но это то же самое, что `f[j]*(j)`, $j < i$, значит по индукционному предположению это обратный элемент. Значит, и рассматриваемый элемент будет обратным.

2. Из условия следует
   $$a^2 - b^2 \equiv 0 \ mod \ n \ \Rightarrow \alpha n = (a-b)(a+b)$$
   Отсюда ясно, что у n и $a-b$ или $a+b$ могут быть общие делители (вероятнее у $a-b$, ведь числа могут быть большими). Поэтому за $\mathcal{O}(\log n)$ найдем $\gcd(n, a-b)$, если он равен единице, найдем $\gcd(n, a+b)$. Потом надо будет поделить число n на найденный НОД (обозначим g), это займет $\mathcal{O}(kl)$, где k, l — длины чисел g, n. Длины можно оценить как $\log n$, поэтому общая асимптотика — $\mathcal{O}(poly(\log n))$

   Подумаем, что может произойти, если $\gcd(n, a \pm b) = n$. Отсюда следует, что $a \pm b = \beta n$, где β — какое-то целое число. Значит $a \pm b \equiv 0 \ mod \ n$, $a \equiv \pm b \ mod \ n$ — но это запрещено условием задачи. Так что такого быть не может

3. Сделаем почти то же самое решето:

   ```
   isprime = True*(n+1)
   smoothness = [None]*(n+1) #массив, в котором будем записывать минимальную гладкость числа
   cnt = 0 #считаем, какое по счету простое число

   for i in range(2, n+1):
       if is_prime[i]:
           cnt += 1 #перешли к следующему по номеру простому числу
           smoothness[j] = cnt #его гладкость - это его порядковый номер
           for j in range(2*i, n+1, i):
               isprime[j] = False
               smoothness[j] = cnt
               #если делится на рассматриваемое простое, то меняем гладкость

   #теперь посчитаем, сколько есть b-гладких чисел строго
   res = [0]*(cnt+1)
   for x in smoothness[1:]:
       res[x] += 1
   ```

```
#учтем, что у числа не одна гладкость
for i in range(cnt):
    res[i+1] += res[i]
```

Что происходит: если в классическом решете мы проверяли числа на простоту, а потом шли вперед, выкалывая числа, которые делятся на найденное простое, то здесь мы не просто выкалываем числа, а записываем в массив порядковый номер текущего их делителя. Поскольку мы идем по возрастанию чисел в решете, в конечном итоге в массиве smoothness будет порядковый номер наибольшего простого делителя для всех чисел вплоть до n (0 в массиве не трогаем). Потом мы посчитаем, сколько чисел есть для каждого такого порядкового номера.
Нужно еще учесть, что если некоторое число b-гладкое, то оно и $b+1$-гладкое, и $b+2$-гладкое и так далее. Это мы учитываем в последнем цикле.
Мы добавили только констатное присваивание и два цикла за $\mathcal{O}(n)$, поэтому общая асимптотика Эратосфена не изменится.

4. $d = e^{-1} \ mod \ \varphi(n)$, то есть $ed = 1 \ mod \ \varphi(n)$. Тогда

$$3d = \alpha\varphi(n) + 1 = \alpha(p-1)(q-1) + 1$$

Рассмотрим функцию

$$f(p,q) = (p-1)(q-1) = (p-1)\left(\frac{n}{p} - 1\right) = n + 1 - p - \frac{n}{p}$$

Ее производная:

$$f'(p) = \frac{n}{p^2} - 1$$

Понятно, что максимума функция достигает при $p = \sqrt{n}$, при этом до этого значения функция возрастает, а после — убывает.
Но если мы сразу начнем подставлять минимально возможное значение $p = 1$, ничего хорошего из неравенства не узнаем. Можем руками проверить числа от 1 до 10 на предмет того, являются ли они делителями, за $\mathcal{O}(\log(n))$. Если ничего не поймали, продолжаем.
Тогда $p, q < \frac{n}{10}$ (p по проверке, q по аналогии — они по сути одно и то же). Тогда можем посмотреть на $f(p)$ при $p = \frac{n}{10}$ и получить нижнюю оценку(n большое, так что смело отбросим константы):

$$f(p) > n + 1 - \frac{n}{10} - 10 \approx \frac{9n}{10}$$

Будет логично предположить, что $d < \varphi(n) < n$, на лекциях при поиске обратного мы хотели, чтобы он был меньше модуля. Тогда:

$$3n > \alpha(p-1)(q-1) + 1 > \frac{9n}{10}\alpha + 1$$

$$\alpha < \frac{10}{3}$$

То есть достаточно проверить $\alpha = 1, 2, 3$, посмотреть, для каких из них получается адекватное целое число. Тогда, зная α, получим

$$t = p + q = \frac{\alpha(n+1) + 1 - 3d}{\alpha}$$

и сможем использовать прием из задачи "Взлом RSA": воспользуемся квадратным уравнением и вычислим p, q

$$p, q = \frac{t \pm \sqrt{t^2 + 4n}}{2}$$

5. Имеем функцию $fact(x)$, которая выдает нам любой делитель a числа n. Понятно, как построить алгоритм, находящий все простые делители: получаем от функции некоторый делитель a, за $\mathcal{O}(poly)$ найдем второй делитель $\frac{n}{a}$, от них тоже запустим $fact$. Если на каком-то шаге получили -1, то это число — простой делитель. Делаем так до тех пор, пока не разложим все.

   Оценим асимптотику: пусть за cn^α находим один нетривиальный делитель. Покажем по индукции, что за $T(n) \leq kn^\alpha$ сумеем найти все.

$$T(n) = T(a) + T(n/a) + cn^\alpha = k(a^\alpha + \left(\frac{n}{a}\right)^\alpha) + cn^\alpha$$

   Рассмотрим $f(a) = k(a^\alpha + \left(\frac{n}{a}\right)^\alpha)$. Это функция, которая достигает минимум в точке $a = \sqrt{n}$ (по сути анализ аналогичный тому, что был сделан в предыдущей задаче), то есть ее наибольшие значения надо искать на краях промежутка, для $a = 2$ или $a = n/2$ (очевидно, большие или меньшие значения a принимать не сможет), при этом по сути это один и тот же случай. Тогда

$$T(n) \leq k(2^\alpha + (n/2)^\alpha) + cn^\alpha = n^\alpha(k(2/n)^\alpha + 1/2^\alpha + c) \leq n^\alpha \cdot k$$

   Чтобы выполнилось неравенство, необходимо выбрать $k > \frac{1/2^\alpha + c}{1-(2/n)^\alpha}$