Студент: Тимур Хабибуллин
Группа: 1
Дата: 5 мая 2022 г.

1. Покажем по индукции. Пусть верно для $i-1$, рассмотрим случай i. Заметим, что `i*(p/i)` = `p - (p%i)`. Возьмем новое посчитанное `f[i]` и умножим его на i, тогда

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

   Раскрывая скобки, получаем много членов, пропорциональных p и один `f[p%i]*(p%i)`, а это по предположению индукции 1 в кольце по модулю p.

2. Так как $a^2 \equiv b^2 \mod n$, то $a^2 - b^2 \equiv 0 \mod n$ и

   $$(a-b)(a+b) = kn.$$

   Тогда рассмотрим g_1 = `gcd(a-b, n)`. Покажем, что g_1 не может быть 1. Пусть это не так, $g_1 = 1$, то посчитаем g_2 = `gcd(a+b, n)`. Так как $(a-b)(a+b) = kn$, то необходимо, чтобы $a+b = \alpha n$, т.е. $g_2 = n$. Но тогда $a+b \equiv 0 \mod n$, т.е. $a \equiv -b \mod n$, что противоречит условию задачи. Аналогично показывается, что g_2 не может быть 1.
   Тогда получается, мы нашли $1 < g_1 < n$, которое является нетривиальным делителем n, тогда второй нетривиальный делитель — n/g_1. Алгоритм работает за $poly(\log(n))$, потому что деление работает за $O(\log(n) * \log(g))$.

3. Заведем массив `min_smooth`, в котором для каждого числа $x \in [0, n]$ запишем, каким минимальным $b-$гладким оно является (ноль - 0-гладкий, любое простое p - p-гладкое; например, 12 - 3-гладкое и тд). Заведем счетчик `b`, в котором будем нумеровать простые числа. Запустим решето Эратосфена. Если число i простое, то счетчик увеличим на 1 и когда будем отмечать числа, кратные i, то будем обновлять `min_smooth`. Это работает за $O(n \log\log n)$. Затем просто посчитаем сколько минимально $b-$гладких чисел получилось и посчитаем кумулятивную сумму, потому что если $a > b$ и число $b-$гладкое, то оно и $a-$гладкое.

```python
n = int(input())
is_prime = [True] * (n + 1)
min_smooth = [0] * (n + 1)
min_smooth[1] = 1
b = 1
for i in range(2, n + 1):
    if is_prime[i]:
        b += 1
        min_smooth[i] = b
        for j in range(2*i, n+1, i):
            is_prime[j] = False
            min_smooth[j] = b
res = [0] * (n + 1)
for x in min_smooth[1:]:
    res[x] += 1
for i in range(2, n+1):
    res[i] += res[i-1]
print(*res)
```

4. По условию $3d \equiv 1 \mod (\phi(n))$ или же

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

Рассмотрим $p, q < 10$, если ни один из этих чисел не является делителем n, то рассмотрим $p, q \geqslant 10$, тогда так как $pq = n$, то $p, q \leqslant n/10$. При этом

$$\varphi(n) = n - p - q - 1 \geqslant n - n/10 - n/10 - 1 \approx 4n/5$$

Тогда так как $d < n$, то

$$3n > 3d > \alpha\varphi(n) + 1 \geqslant \alpha\frac{4n}{5} + 1$$

$$\alpha < \frac{15}{4} < 4$$

Получается что надо перебрать $\alpha = 1, 2, 3$. Тогда для данного α мы получаем уравнение на сумму

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

Учитывая, что $pq = n$, получим квадратное уравнение, которое сможем решить.

5. Пусть умеем за cn^α находить один нетривиальный делитель, тогда $O(poly\log(n))$ находим второй делитель (это не влияет на асимптотику). Покажем, что разложим на множители за $T(n) = kn^\alpha$ Пусть получили a, тогда

$$T(n) = T(a) + T(n/a) + cn^\alpha = k(a^\alpha + (n/a)^\alpha) + cn^\alpha$$

Расмотрим функцию $f(a) = a^\alpha + (n/a)^\alpha$. Если исследовать эту функцию (взять 2 производные и посмотреть в вольфраме), то она достигает единственный минимум в $a = n^{1/2}$. Тогда так $2 \leqslant a \leqslant n/2$, то максимум будет достигаться на краях промежутка, т.е. при $a = 2$ или $a = n/2$. Тогда

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

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

$Q, K, V \in \mathbb{R}^{N \times d_{model}}$

$W_i^Q, W_i^K, W_i^V \in \mathbb{R}^{d_{model} \times d}$

$QW_i^Q, KW_i^K, VW_i^V \in \mathbb{R}^{N \times d}$

$$\mathrm{A} = \mathrm{softmax}\left(\frac{QW_i^Q(KW_i^K)^T}{\sqrt{d}}\right) \in \mathbb{R}^{N \times N}$$

d
Time(Transformer) $= O(N^2 \cdot d)$
Time(Fastformer) $= O(N \cdot d)$
param(Transformer)=