Домашняя работа 1

Александр Петровский, M3239

May 2018

Задача 1

Известно, что $\varsigma(s) = \sum\limits_{n=1}^{\infty} \frac{1}{n^s}$. Нужно доказать справедливость следующего тождества $\varsigma(s) = \prod\limits_{p \in P} (1 - \frac{1}{p^s})^{-1}$.

Рассмотрим один множитель из бесконечного произведения: $A_p = (1 - \frac{1}{p^s})^{-1} = (\frac{p^s-1}{p^s})^{-1} = \frac{p^s}{p^s-1} = \frac{1}{1-\frac{1}{p^s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + ... = 1 + p^{-s} + p^{-2s} + p^{-3s} + ... = \sum\limits_{n=0}^{\infty} p^{-ns}$

Понятно, что произведение $\prod\limits_{p \in P} A_p$ даст все возможные комбинации простых чисел в степени кратной $-s$. Например для двух простых чисел p и q: $A_p * A_q = (1 + p^{-s} + p^{-2s} + p^{-3s} + ...) * (1 + q^{-s} + q^{-2s} + q^{-3s} + ...) = 1 * (1 + q^{-s} + q^{-2s} + q^{-3s} + ...) + p^{-s} * (1 + q^{-s} + q^{-2s} + q^{-3s} + ...) + ...$ Тогда очевидно, что поскольку мы рассматриваем все простые числа во всех степенях кратных $-s$, то их комбинации дадут все целые положительные числа в степени, которая также равна $-s$. Поскольку каждой число имеет единственную факторизацию, то склеек не будет. Но это значит, что мы получили $\varsigma(s)$.

Задача 2

Требуется показать, что $\sum\limits_{d|n} \varphi(d) = n$.

1. Пусть n - простое число. Тогда у него есть две делителя n и 1. $\varphi(n) + \varphi(1) = (n-1) + 1 = n$.

2. Пусть n - составное. Тогда будем действовать по индукции.

   - База: Для n = 1, 2, 3 мы показали, что это верно в пункте 1. Рассмотрим n = 4. Его делители - 1, 2, 4. $\varphi(1) + \varphi(2) + \varphi(4) = 1 + 1 + 2 = 4$.
   - Шаг: Пусть мы доказали для всех чисел меньших либо равных n. Пусть $d_1, d_2, d_3, ...d_k$ - делители числа n. Рассмотрим число $m = n * q$, где q - простое число. Рассмотрим два случая

(a) q не входит в разложение на простые числа n. Тогда делителями числа m будет набор $d_1, d_2, ..., d_k, q*d_1, q*d_2, ..., q*d_k$ при этом $gcd(q, d_i) = 1$. Тогда рассмотрим сумму : $\varphi(d_1) + \varphi(d_2) + ...\varphi(d_k) + \varphi(q*d_1) + \varphi(q*d_2) + ... + \varphi(q*d_k) = n + \varphi(q)*\varphi(d_1) + \varphi(q)*\varphi(d_2) + ... + \varphi(q)*\varphi(d_k) = n + \varphi(q)*(n) = n*(1+\varphi(q)) = n*(1+(q-1)) = n*q = m$.

(b) q входит в разложение на простые числа n. Тогда аналогично пункту (a) построим набор делителей $d_1, d_2, ..., d_k, q*d_1, q*d_2, ..., q*d_k$. Теперь в наборе делителей числа m, который мы построили, один делитель может встречаться дважды. Это будет случаться, если q уже делило какой-то делитель. Рассмотрим набор таких делителей $d_{i_1}, d_{i_2}, ..., d_{i_l}$, который будет порождать новые делители, т.е. $d_{i_1} * q$ - уже не будет делителем n. Легко показать, что $\varphi(d_{i_1} * q) = q * \varphi(d_{i_1})$. Действительно, $\varphi(d_{i_1} * q) = [r$ - максимальная степень вхождения q в $n] = \varphi(t*q^r*q) = [gcd(t,q) = 1] = \varphi(t*q^{r+1}) = (q^{r+1} - q^r)\varphi(t)$, где t - делитель числа n/q^r, а значит, что этот набор состоит из делителей числа n/q^r домноженный на q^r. Теперь рассмотрим сумму по делителям: $\varphi(d_1) + \varphi(d_2) + ...\varphi(d_k) + \varphi(q*d_{i_1}) + \varphi(q*d_{i_2}) + \varphi(q*d_{i_l}) = n + q\sum_{j=1}^{l}\varphi(d_{i_j}) = n + q\sum_{j=1}^{l}(q-1)q^{r-1}\varphi(d_{i_j}/q^r) = n + q(q-1)q^{r-1}\sum_{j=1}^{l}\varphi(d_{i_j}/q^r) =$ [по предположению индукции $\sum_{j=1}^{l}\varphi(d_{i_j}/q^r) = n/q^r] = n + q(q-1)q^{r-1} * n/q^r = n + (q-1)n = nq = m$

Задача 3

$n = pq$ Пусть $q > p$. Тогда алгоритм очевиден. Пусть $x = sqrt(n)$. Тогда $q >= x$ $x >= p$. Используя это напишем алгоритм.

```
fun fact(n)
    x = sqrt(n)
    for i in 0...infinity
        if (n % (x + i) == 0)
            return n/(x + i), (x + i)
```

Корень можно посчитать бинпоиском за $poly(logn)$, собственно, как и деление. Очевидно, что этот алгоритм сделает $<= |p - q|$ шагов.