1. Вступление.

Хорошо известно, что количество делителей числа N нечётно тогда и только тогда, когда N – полный квадрат. Но количество делителей числа N – это количество упорядоченных наборов из двух чисел, произведение которых равно N. С учётом этого, попробуем обобщить факт про чётность количества делителей.

Количество способов представить число N как произведение чисел упорядоченного набора из m элемантов будем обозначать через π_N^m. Несложно понять, что если $N = {p_1}^{\alpha_1}{p_2}^{\alpha_2} \cdot \ldots \cdot {p_n}^{\alpha_n}$, то π_N^m – это количество способов разложить по m пронумерованным коробкам α_1 одинаковых шаров, на которых написано p_1, а также α_2 одинаковых шаров, на которых написано p_2, и так далее, α_n одинаковых шаров, на которых написано p_n. Через метод шаров и перегородок мы понимаем, что количество способов разложить α_i одинаковых шаров по m пронумерованным ящикам – это

$$C_{\alpha_i+m-1}^{\alpha_i} = \frac{m(m+1)(\ldots)(m+\alpha_i-1)}{\alpha_i!} = \frac{m}{1} \cdot \frac{m+1}{2} \cdot \ldots \cdot \frac{m+\alpha_i-1}{\alpha_i}$$

Эти числа нужно перемножить по всем i, чтобы получить π_N^m. Если t_i – это количество чисел среди α_j, не меньших i, то дробь $\frac{m+i-1}{i}$ встретится в произведении ровно t_i раз. Отсюда формула:

$$\pi_N^m = \left(\frac{m}{1}\right)^{t_1} \left(\frac{m+1}{2}\right)^{t_2} \cdot \ldots \cdot \left(\frac{m+i-1}{i}\right)^{t_i} \cdot \ldots \cdot \left(\frac{m+k-1}{k}\right)^{t_k}$$

Число k в этой формуле можно взять любым, не меньшим $\max\limits_{1 \le i \le n} \alpha_i$ – если k будет строго больше этой величины, произведение просто будет домножено на несколько единиц, т.к. все t_j, где $j > \max\limits_{1 \le i \le n} \alpha_i$, нулевые.

Теперь, когда у нас есть формула для вычисления π_N^m, мы можем сформулировать и доказать следующее утверждение:

Теорема. Количество упорядоченных наборов p чисел (p простое), произведение которых равно $N > 1$, не делится на p тогда и только тогда, когда $N = z^p, z \in \mathbb{N}$; к тому же, оно принимает только остатки 0 и 1 от деления на p.

Эта теорема является прямым обобщением рассмотренного ранее утверждения про количество делителей числа. Мы приведём два её доказательства: комбинаторное и через прямой подсчёт.

Комбинаторное доказательство. Все представления числа N в виде произведения p чисел объединим в группы по p элементов: в каждой группе представления, которые можно получить циклическим сдвигом друг из друга. Если в представлении не все множители равны, циклическим сдвигом из этого представления можно получить p различных представлений. В самом деле, если после сдвига на n получилось то же представление, то первое число в представлении такое же, как под номером $n+1$, такое же, как под номером $2n+1$, и так далее, а поскольку p простое, эти индексы по модулю p охватывают все остатки, то есть все числа в представлении одинаковые. В наши группы, таким образом, нельзя включить только такое представление, где все p множителей равны. Оно есть тогда и только тогда, когда N – это степень p некоторого числа, а в таком случае в группы по p мы не включили только одно представление.

Доказательство прямым подсчётом. В формуле

$$\pi_N^p = \left(\frac{p}{1}\right)^{t_1} \left(\frac{p+1}{2}\right)^{t_2} \left(\frac{p+2}{3}\right)^{t_3} \cdot \ldots \cdot \left(\frac{p+k-1}{k}\right)^{t_k}$$

разделим все множители на группы по p множителей, идущих по порядку. Мы можем это сделать, так как мы можем выбрать любое k, начиная с некоторого. Любая такая группа в таком случае выглядит так:

$$\left(\frac{np}{(n-1)p+1}\right)^{t_{(n-1)p+1}} \left(\frac{np+1}{(n-1)p+2}\right)^{t_{(n-1)p+2}} \cdot \ldots \cdot \left(\frac{np+p-1}{np}\right)^{t_{np}}$$

Из всех множителей в числителе и знаменателе на p делится только np. При этом $t_{np} \leq t_{(n-1)p+1}$, поэтому при раскрытии скобок в каждой группе p окажется в неотрицательной степени. А во всём произведении p будет в нулевой степени тогда и только тогда, когда $t_{np} = t_{(n-1)p+1} \forall n$. В таком случае, если $N = p_1^{\alpha_1} p_2{}^{\alpha_2} \cdot \ldots \cdot p_m{}^{\alpha_m}$, то количество α_i, не меньших np, и количество α_j, не меньших $(n-1)p+1$, одинаково, значит, нет никаких α_i между $(n-1)p$ и kp (не включая концы), значит, все α_i делятся на p, то есть N – степень p натурального числа. Но в таком случае в каждой группе все степени скобок равны, поэтому после сокращения np и в числителе, и в знаменателе по модулю p стоит произведение всех остатков от деления на p, кроме 0, и вся дробь возведена в некоторую степень. Разумеется, после выполнения деления останется единица. Мы доказали необходимость, достаточность доказывается аналогично – просто применяем те же шаги в обратном порядке.