Хорошо известно, что количество делителей натурального числа N нечётно тогда и только тогда, когда N – полный квадрат. Но количество делителей N – это количество упорядоченных наборов 2 натуральных чисел, произведение которых равно N. Поэтому мы будем обобщать факт про чётность количества делителей до теорем про количество таких упорядоченных наборов. Одним из таких обобщений будет следующая теорема.

Теорема 1. Для любых простого числа p и натурального числа N выполнено следующее: количество упорядоченных наборов p натуральных чисел, произведение которых равно N, не делится на p тогда и только тогда, когда $N = z^p, z \in \mathbb{N}$. Более того, это количество для любых простого p и натурального N принимает остаток 0 или 1 от деления на p.

Доказательство теоремы 1. Упорядоченные наборы p натуральных чисел, произведение которых равно N, объединим в группы по p элементов: в каждой группе наборы, которые можно получить циклическим сдвигом друг из друга. Если в наборе не все множители равны, циклическим сдвигом из этого представления можно получить p различных наборов. В самом деле, если после сдвига на n получился тот же набор, то первое число в этом наборе 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 наборе одинаковые. В наши группы, таким образом, нельзя включить только такой упорядоченный набор, в котором все p чисел равны. А такой набор есть тогда и только тогда, когда N – это степень p некоторого числа, а в таком случае в группы по p мы не включили только один набор, поэтому остаток от деления количества наборов на p равен 1, ЧТД.

Доказательство, приведённое выше, комбинаторное. Ниже мы приведём ещё одно доказательство теоремы 1, на этот раз опирающееся на прямое вычисление. Но для этого необходимо вывести формулу для рассматриваемого нами количества упорядоченных наборов.

Количество упорядоченных наборов m натуральных чисел, произведение которых равно N, будем обозначать π_N^m. Несложно понять, что если $N = {p_1}^{\alpha_1}{p_2}^{\alpha_2} \cdot \ldots \cdot {p_n}^{\alpha_n}$, где p_i – различные простые числа, 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 от 1 до n, 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 таком произведении ровно t_i раз. Отсюда формула:

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

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. Руководствуясь формулой, взятой в рамку, также можно доказать теорему 1.

Доказательство теоремы 1 прямым подсчётом. Пусть $N = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdot\ldots\cdot{p_n}^{\alpha_n}$, где p_i – различные простые числа, t_i –количество чисел среди α_j, не меньших i. Тогда применима выведенная формула:

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

Разделим в этой формуле 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:

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

Из всех множителей в числителе и знаменателе на p делится только kp. Более того, поскольку $t_{kp}\le t_{(k-1)p+1}$, то при раскрытии скобок в каждой из групп число p окажется в неотрицательной степени. А во всём произведении p будет в нулевой степени тогда и только тогда, когда $t_{kp} = t_{(k-1)p+1}\forall k$. В таком случае количество α_i, не меньших kp, и количество α_j, не меньших $(k-1)p+1$, одинаково, значит, нет никаких α_i между $(k-1)p$ 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 kp 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. Если же $\pi_N^p \vdots p$, то в какой-то из групп при раскрытии скобок kp будет в строго положительной степени, поэтому $t_{kp} < t_{(k-1)p+1}$ для некоторого k, а в таком случае N не будет степенью p натурального числа, т.к. найдётся i такой, что α_i не делится на p.

Итак, π_N^p не делится на p тогда и только тогда, когда $N = z^p, z\in\mathbb{N}$, причём π_N^p принимает остаток 0 или 1 от деления на p, что и требовалось доказать.

Теорема 1 обобщает исходный факт про чётность количества делителей до факта про π_N^p для простых p. Далее мы выведем несколько теорем для π_N^m, где m – произвольное (возможно, составное) натуральное число.

Как мы замечали ранее, если $N = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdot\ldots\cdot{p_n}^{\alpha_n}\in\mathbb{N}$, где p_i – различные простые числа, 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. Отсюда понятно, что для взаимно простых N_1 и N_2 верно $\pi_{N_1N_2}^m = \pi_{N_1}^m\pi_{N_2}^m$ – мультипликативность. Это несколько упростит нашу дальнейшую работу.

Пусть $N = {p_1}^{\alpha_1}{p_2}^{\alpha_2} \cdot \ldots \cdot {p_n}^{\alpha_n} \in \mathbb{N}$, где p_i – различные простые числа, p – некоторое простое число. Тогда по нашей формуле:

$$\pi^m_{({p_i}^{\alpha_i})} = \left(\frac{m}{1}\right)\left(\frac{m+1}{2}\right)\left(\frac{m+2}{3}\right) \cdot \ldots \cdot \left(\frac{m+\alpha_i-1}{\alpha_i}\right)$$

$$\mathrm{ord}_p\left(\pi^m_{({p_i}^{\alpha_i})}\right) = \mathrm{ord}_p\left(\left(\frac{m}{1}\right)\left(\frac{m+1}{2}\right)\left(\frac{m+2}{3}\right) \cdot \ldots \cdot \left(\frac{m+\alpha_i-1}{\alpha_i}\right)\right)$$

$$\mathrm{ord}_p\left(\pi^m_{({p_i}^{\alpha_i})}\right) = \sum_{j=1}^{\alpha_i}\left(\mathrm{ord}_p(m+j-1) - \mathrm{ord}_p(j)\right)$$

$$\mathrm{ord}_p\left(\pi^m_{({p_i}^{\alpha_i})}\right) = \sum_{j=1}^{\alpha_i}\mathrm{ord}_p(m+j-1) - \sum_{j=1}^{\alpha_i}\mathrm{ord}_p(j)$$

Если $\alpha_i \geq m$, то в этих суммах есть одинаковые слагаемые, от которых мы можем избавиться, получив формулу ниже:

$$\mathrm{ord}_p\left(\pi^m_{({p_i}^{\alpha_i})}\right) = \sum_{j=\alpha_i+2-m}^{\alpha_i}\mathrm{ord}_p(m+j-1) - \sum_{j=1}^{m-1}\mathrm{ord}_p(j)$$

Легко понять, что формула выше выполнена не только для случая $\alpha_i \geq m$: если $\alpha_i = m-1$, то суммы не изменились, а если $\alpha_i < m-1$, мы добавили в каждую из сумм несколько одинаковых слагаемых. Перепишем первую сумму в несколько другом виде:

$$\boxed{\mathrm{ord}_p\left(\pi^m_{({p_i}^{\alpha_i})}\right) = \sum_{j=1}^{m-1}\mathrm{ord}_p(\alpha_i+j) - \sum_{j=1}^{m-1}\mathrm{ord}_p(j)}$$

Формулу выше мы позже используем для вычисления $\mathrm{ord}_p\left(\pi^m_{({p_i}^{\alpha_i})}\right)$. Но прежде, чем это произойдёт, мы немного изменим её вид для доказательства других теорем:

$$\mathrm{ord}_p\left(\pi^m_{({p_i}^{\alpha_i})}\right) = \sum_{j=0}^{m-1}\mathrm{ord}_p(\alpha_i+j) - \sum_{j=1}^{m}\mathrm{ord}_p(j) + \mathrm{ord}_p m - \mathrm{ord}_p\alpha_i$$

В этом выражении можно доказать, что разность сумм неотрицательна:

$$\sum_{j=0}^{m-1}\mathrm{ord}_p(\alpha_i+j) - \sum_{j=1}^{m}\mathrm{ord}_p(j) = \mathrm{ord}_p\left(\frac{\alpha_i(\alpha_i+1)(\ldots)(\alpha_i+m-1)}{m!}\right) = \mathrm{ord}_p\left(C^m_{\alpha_i+m-1}\right) \geq 0$$

Подставляя это неравенство, получаем, что

$$\boxed{\mathrm{ord}_p\left(\pi^m_{({p_i}^{\alpha_i})}\right) \geq \mathrm{ord}_p m - \mathrm{ord}_p\alpha_i}$$

Значит, если $\pi^m_{(p_i{}^{\alpha_i})}$ не делится на простое число p, то $0 \geq \mathrm{ord}_p m - \mathrm{ord}_p \alpha_i$, что равносильно $\mathrm{ord}_p \alpha_i \geq \mathrm{ord}_p m$. Используя это, сформулируем и докажем две теоремы.

Теорема 2. Если для натуральных m и N число π^m_N взаимно просто с m, то $N = z^m, z \in \mathbb{N}$.

Доказательство теоремы 2. Пусть для натуральных m и N число π^m_N взаимно просто с m, где $N = {p_1}^{\alpha_1}{p_2}^{\alpha_2} \cdot \ldots \cdot {p_n}^{\alpha_n}$, p_i – различные простые числа. Тогда π^m_N не делится на любой простой делитель p числа m. Значит, для любого такого p число $\pi^m_{(p_i{}^{\alpha_i})}$ не делится на p для любого i из-за мультипликативности, поэтому $\mathrm{ord}_p \alpha_i \geq \mathrm{ord}_p m \forall i \forall p | m$. Отсюда следует, что $\alpha_i \vdots m \forall i$, поэтому $N = z^m, z \in \mathbb{N}$, ЧТД.

Теорема 3. Если для натуральных m и N число π^m_N не делится на m, то существует простое $p | m$ такое, что $N = z^p, z \in \mathbb{N}$.

Доказательство теоремы 3. Пусть для натуральных m и N число π^m_N не делится на m, где $N = {p_1}^{\alpha_1}{p_2}^{\alpha_2} \cdot \ldots \cdot {p_n}^{\alpha_n}$, p_i – различные простые числа. Тогда $\mathrm{ord}_p(\pi^m_N) < \mathrm{ord}_p m$ для некоторого простого p, являющегося делителем m. Тогда $\mathrm{ord}_p\left(\pi^m_{(p_i{}^{\alpha_i})}\right) < \mathrm{ord}_p m \forall i$ из-за мультипликативности. Подставим это в неравенство $\mathrm{ord}_p\left(\pi^m_{(p_i{}^{\alpha_i})}\right) \geq \mathrm{ord}_p m - \mathrm{ord}_p \alpha_i$ и получим $\mathrm{ord}_p m > \mathrm{ord}_p m - \mathrm{ord}_p \alpha_i \forall i$, откуда $\mathrm{ord}_p \alpha_i > 0 \forall i$, поэтому число N – точная p-ая степень натурального числа, ЧТД.

Теоремы 2 и 3 утверждают, что некоторое условие выполнено, если π^m_N не делится на натуральное m или даже взаимно просто с ним. Следует подойти к проблеме и с другой стороны: например, доказать, что π^m_N не делится на m, если выполнено некоторое условие.

Теорема 4. Если $m \in \mathbb{N}$, $N = q^{np^\alpha}$, где p и q простые, $n \in \mathbb{N}$, $\alpha \geq \log_p m$ – натуральное, то π^m_N не делится на p.

Доказательство теоремы 4. Пусть дано некоторое натуральное m, $N = q^{np^\alpha}$, где p и q простые, $n \in \mathbb{N}$, $\alpha \geq \log_p m$ – натуральное. Тогда по выведенной нами ранее формуле

$$\mathrm{ord}_p(\pi^m_N) = \sum_{j=1}^{m-1} \mathrm{ord}_p(np^\alpha + j) - \sum_{j=1}^{m-1} \mathrm{ord}_p(j)$$

Поскольку $\alpha \geq \log_p m$, то $p^\alpha \geq m$, поэтому $\mathrm{ord}_p(np^\alpha) \geq \mathrm{ord}_p(p^\alpha) > \mathrm{ord}_p(j)$ при j от 1 до $m - 1$. Поэтому $\mathrm{ord}_p(np^\alpha + j) = \mathrm{ord}_p(j)$, откуда $\mathrm{ord}_p(\pi^m_N) = 0$, поэтому π^m_N не делится на p, ЧТД.

Используя теорему 4, мы можем улучшить результат теоремы 2 для чисел, являющихся степенью простого:

Теорема 2.1. Если натуральное число m – степень простого, $N \in \mathbb{N}$, то π^m_N взаимно просто с m тогда и только тогда, когда $N = z^m, z \in \mathbb{N}$.

Доказательство теоремы 2.1. Необходимость теоремы 2.1 выполнена по теореме 2, поэтому докажем достаточность. Пусть $m = p^\alpha$, где p – простое, α – целое неотрицательное.

Если $N = z^m, z \in \mathbb{N}$, то $N = z^{p^\alpha}$, где $\alpha = \log_p m$, поэтому применима теорема 4. Она утверждает, что π_N^m не делится на p, поэтому π_N^m взаимно просто с m, ЧТД.