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 представлений N в виде произведения двух чисел (с учётом порядка сомножителей). Это позволяет выдвинуть гипотезу.

Гипотеза 1. Количество представлений числа N в виде произведения m чисел не делится на m тогда и только тогда, когда $N = t^m, t \in \mathbb{N}$.

К сожалению, гипотеза неверна. Так, число 9 можно десятью способами представить в виде произведения четырёх чисел, но число 9 не является точной четвёртой степенью, хотя количество представлений на 4 не делится. В обратную сторону утверждение тоже неверно: позже мы получим формулу для количества таких представлений, из которой сразу будет следовать, что число $64 = 2^6$ можно представить в виде произведения шести чисел $462 = 6 \cdot 77$ способами.

Тем не менее, эта гипотеза в некоторых случаях работает: позже мы её докажем для простых m (см. теорему 1). Но в случае простых чисел фразы «не делится на m» и «взаимно просто с m» обозначают одно и то же, поэтому имеет смысл попробовать изменить формулировку гипотезы.

Гипотеза 2. Количество представлений числа N в виде произведения m чисел взаимно просто с m тогда и только тогда, когда $N = t^m, t \in \mathbb{N}$.

Числа 64 и 6 остаются контрпримерами: количество представлений числа 64 в виде произведения 6 чисел делится на 6, но при этом не взаимно просто с шестью. Однако необходимость оказывается верной (см. теорему 2). Кроме того, достаточность верна для всех степеней простых чисел (см. теорему 2.1).

2. Вычисление количества представлений.

Количество способов представить число N как произведение чисел упорядоченного набора из m чисел 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.

Используя эту формулу, мы можем посчитать число π_{64}^6, на которое ссылались ранее: для него $t_1 = t_2 = \cdots = t_6 = 1$, $t_7 = t_8 = \cdots = 0$, что мы подставляем в формулу выше и получаем $\pi_{64}^6 = \frac{6}{1} \cdot \frac{7}{2} \cdot \frac{8}{3} \cdot \frac{9}{4} \cdot \frac{10}{5} \cdot \frac{11}{6} = 6 \cdot 7 \cdot 11 = 462$.

Если раскрыть все скобки в полученной нами формуле для π_N^m, в числителе и знаменателе будет порой стоять много одинаковых чисел. Поэтому иногда нам будет удобнее частично сократить числитель и знаменатель, в результате чего мы придём к такой формуле:

$$\pi_N^m = \frac{m^{t_1 - t_m}(m+1)^{t_2 - t_{m+1}} \cdot \ldots \cdot (m+k-1)^{t_k - t_{m+k-1}}}{1^{t_1} \cdot 2^{t_2} \cdot \ldots \cdot (m-1)^{t_{m-1}}}$$

π_N^2 – это количество представлений числа N в виде произведения двух чисел, то есть количество делителей числа N. Подставим $m = 2$ в формулу:

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

Число $t_i - t_{i+1}$ – это количество чисел α_j, равных i. Поэтому в традиционной записи количества делителей числа $d(N) = (\alpha_1 + 1)(\alpha_2 + 1)(\ldots)(\alpha_n + 1)$ скобка, равная $i + 1$, встречается ровно $t_i - t_{i+1}$ раз, поэтому в этих двух произведениях перемножаются одни и те же числа. Более того, из нашей формулы видно, что π_N^2 нечётно тогда и только тогда, когда все чётные числа возводятся в нулевые степени, то есть когда $t_1 = t_2$, $t_3 = t_4$, и так далее, что и означает, что число N – полный квадрат. Далее мы будем обобщать это утверждение для произвольного m.

3. Обобщение для простых m.

<u>Теорема 1</u>. Количество представлений числа N в виде произведения p чисел (p простое) не делится на p тогда и только тогда, когда $N = z^p, z \in \mathbb{N}$, а в таком случае это количество представлений сравнимо с единицей по модулю p.

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

<u>Комбинаторное доказательство</u>. 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 <u>различных</u> 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.

4. Обобщения для составных m. Часть 1.

Пусть p – некоторое простое число. Тогда

$$\operatorname{ord}_p(\pi_N^m) = \operatorname{ord}_p\left(\left(\frac{m}{1}\right)^{t_1}\left(\frac{m+1}{2}\right)^{t_2}\left(\frac{m+2}{3}\right)^{t_3}\cdot\ldots\cdot\left(\frac{m+n-1}{n}\right)^{t_n}\right)$$

$$\operatorname{ord}_p(\pi_N^m) = \sum_{i=1}\left(\left(\operatorname{ord}_p(m+i-1) - \operatorname{ord}_p(i)\right)t_i\right)$$

Как мы замечали ранее, 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. Отсюда понятно, что для взаимно простых N_1 и N_2 верно $\pi_{N_1 N_2}^m = \pi_{N_1}^m \pi_{N_2}^m$ – мультипликативность. Поэтому нам достаточно уметь вычислять $\operatorname{ord}_p\left(\pi_{(p_i{}^{\alpha_i})}^m\right)$:

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

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

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

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

Легко понять, что формула выше работает 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:

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

Формулу выше мы будем использовать для вычисления $\operatorname{ord}_p\left(\pi^m_{({p_i}^{\alpha_i})}\right)$. Но для наших целей её необходимо изменить:

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

В этом выражении можно доказать, что разность сумм неотрицательна:

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

Подставляя это неравенство, получаем, что

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

То есть, если $\pi^m_{({p_i}^{\alpha_i})}$ не делится на простое число p, то $0 \geq \operatorname{ord}_p m - \operatorname{ord}_p \alpha_i$, то есть $\operatorname{ord}_p \alpha_i \geq \operatorname{ord}_p m$. Из этого следует два важных утверждения.

Во-первых, если π^m_N взаимно просто с m, где $N = {p_1}^{\alpha_1}{p_2}^{\alpha_2} \cdot \ldots \cdot {p_n}^{\alpha_n}$, то π^m_N не делится на любой простой делитель m (обозначим один из них через p), тогда $\pi^m_{({p_i}^{\alpha_i})}$ не делится на p для любого i из-за мультипликативности, поэтому $\operatorname{ord}_p \alpha_i \geq \operatorname{ord}_p m \forall i$. Поскольку это выполнено для любого простого делителя m, можно сделать вывод, что $\alpha_i \vdots m$.

Теорема 2. Если количество представлений числа N в виде произведения m чисел взаимно просто с m, то $N = z^m, z \in \mathbb{N}$.

Во-вторых, если π_N^m не делится на m, то π_N^m не делится на какой-то простой делитель m (обозначим его через p), тогда $\pi_{(p_i{}^{\alpha_i})}^m$ не делится на p для любого i из-за мультипликативности, поэтому $\mathrm{ord}_p \alpha_i \geq \mathrm{ord}_p m \forall i$, поэтому число N – точная p-ая степень натурального числа.

Теорема 3. Если количество представлений числа N в виде произведения m чисел не делится на m, то $N = z^p, z \in \mathbb{N}, m \vdots p$ (p простое).

5. Обобщения для составных m. Часть 2.

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

Пусть дано некоторое m, $N = q^{np^\alpha}$, $\alpha \geq \log_p m$ (p и q простые, $n \in \mathbb{N}$). Тогда по выведенной нами ранее формуле

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

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 $\mathrm{ord}_p(\pi_N^m) = 0$, поэтому π_N^m не делится на p. Отсюда вытекает теорема 4:

Теорема 4. Если $N = a_1{}^{p^{\alpha_1}} a_2{}^{p^{\alpha_2}} \cdot \ldots \cdot a_k{}^{p^{\alpha_k}}$, $\alpha_i \geq \log_p m$ (p простое), то π_N^m взаимно просто с p.

Числа $a_1, a_2, \ldots, a_k$ в теореме 4 необязательно простые: утверждение теоремы 4 следует из рассуждений выше и для составных $a_1, a_2, \ldots, a_k$. Если мы выберем число p делителем числа m, то мы получим достаточное условие того, что π_N^m не делится на m.

Пусть $m = p_1^{\alpha_1} p_2{}^{\alpha_2} \cdot \ldots \cdot p_k{}^{\alpha_k}$, $\beta_i \geq \log_{p_i} m$, $N = q^{p_1{}^{\beta_1} p_2{}^{\beta_2} \cdot \ldots \cdot p_k{}^{\beta_k}}$. Тогда по теореме 4 $\text{НОД}(\pi_N^m; m) = 1$:

Теорема 4.1. $\forall m \exists N: \text{НОД}(\pi_N^m; m) = 1$.

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

Теорема 2.1. Если число m – степень простого, то $\text{НОД}(\pi_N^m; m) = 1 \Leftrightarrow N = z^m$.

В самом деле, необходимость выполнена по теореме 2, а достаточность следует из теоремы 4.