1 MM181

Докажем, что для любого числа $k \geq 0$, существует число n такое, что при делении на все числа меньшие или равные n, остаток k встречается чаще всего.

Обозначим $\sigma(n, a)$ число делителей n больших a. Легко видеть, что количество остатков равных a при делении числа n на все числа от 1 до n равно $\sigma(n-a, a)$. Соответственно, нам нужно найти такое число n, что $k = \mathrm{argmax}_{0\leq a<n}\sigma(n-a, a)$.

Назовем число n граничным, если для любого числа $m < n$ выполнено $\sigma(m) < \sigma(n)$. Обозначим p_n n-тое простое число.

Заметим, что любое граничное число имеет вид $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$, где $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_s > 0$. В противном случае можно либо заменить какой-либо простой делитель на меньший и получить меньшее число с таким же числом делителей, либо поменять степени простых делителей местами с тем же результатом.

Лемма 1 *Для разложения граничного числа $N = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$ на простые множители выполнены неравенства*

$$p_i^{\alpha_i} > \sqrt{p_n},$$
$$p_i^{\alpha_i} < p_{n+1}^4.$$

Доказательство. Обозначим β_i максимальное целое число такое, что $p_i^{\beta_i} \leq p_n$. Если $p_i^{\beta_i} \leq \sqrt{p_n}$, то $p_i^{2\beta_i} \leq p_n$, но поскольку $2\beta_i > \beta_i$, мы получаем противоречие с определением β_i. Следовательно, выполнено неравенство $p_i^{\beta_i} > \sqrt{p_n}$. Предположим, что $\alpha_i < \beta_i$ для некоторого $i < n$. Рассмотрим число $N\frac{p_i^{\beta_i}}{p_n}$. Это число меньше, чем N, а количество его делителей не меньше $\frac{\alpha_i+\beta_i+1}{2(\alpha_i+1)}\sigma(N) \geq \frac{\alpha_i+(\alpha_i+1)+1}{2(\alpha_i+1)}\sigma(N) = \sigma(N)$, получили противоречие. Значит $p_i^{\alpha_i} \geq p_i^{\beta_i} > \sqrt{p_n}$ для $i < n$. Для $i = n$ предыдущее неравенство очевидно. Первое утверждение леммы доказано.

Обозначим γ_i наименьшее целое число такое, что $p_i^{\gamma_i} \geq p_{n+1}$. Если $p_i^{\gamma_i} \geq p_{n+1}^2$, то $p_i^{[(\gamma_i+1)/2]} \geq p_{n+1}$. Поскольку $\gamma_i > 1$, то $\gamma_i > [(\gamma_i+1)/2]$ т.е. число γ_i не является наименьшим. Отсюда получаем, что $p_i^{\gamma_i} < p_{n+1}^2$. Предположим, что $\alpha_i > 2\gamma_i$. Рассмотрим число $N\frac{p_{n+1}}{p_i^{\gamma_i}}$. Это число меньше чем N (равенство $p_i^{\gamma_i} = p_{n+1}$ не возможно при $i \leq n$), а количество его делителей равно $\frac{2(\alpha_i-\gamma_i+1)}{\alpha_i+1}\sigma(N) > \frac{\alpha_i+(\alpha_i-2\gamma_i)+1}{\alpha_i+1}\sigma(N) > \frac{\alpha_i+1}{\alpha_i+1}\sigma(N) = \sigma(N)$, получаем противоречие. Значит $p_i^{\alpha_i} \leq p_i^{2\gamma_i} < p_{n+1}^4$. Второе утверждение леммы доказано.□

Обозначим G_n такое граничное число, что его максимальный простой делитель равен p_n, а у всех меньших граничных чисел максимальный простой делитель меньше p_n. Такое число может существовать не при всех n. Однако, поскольку граничных чисел бесконечно много, а граничное число с максимальным простым делителем p_n ограничено числом p_{n+1}^{4n} по Лемме 1, то существует бесконечно много чисел G_n.

Обозначим $C_1(k)$ наименьшее число n при котором $p_n \geq k^2$. Поскольку при разложении G_n, $n \geq C_1(k)$ на множители мы имеем $p_i^{\alpha_i} > \sqrt{p_n} \geq k$, то в этом случае$G_n$ делится на все числа от 1 до k. Обозначим $C_2(k)$ наименьшее число n при котором $p_n > 2^{4k-1}$.

Лемма 2 *Если $n \geq C_1(k)$ и $n \geq C_2(k)$, то $\sigma(G_n+s) < \sigma(G_n)/2$ для $1 \leq s \leq k$.*

Доказательство. Поскольку G_n делится на все числа от 1 до k, то $\sigma(G_n+s) = \sigma(s)\sigma\left(\frac{G_n}{s}+1\right)$. Обозначим $N_1 = \frac{G_n}{s}+1$. Поскольку $p_i^{\alpha_i} > k$, то число $\frac{G_n}{s}$ делится на все простые числа от p_1 до p_n. Значит наименьший простой делитель p_s числа N_1 больше чем p_n. Рассмотрим целое число $N_2 = 2^{4k-1}N_1/p_s$. Мы можем оценить $N_1 \le G_n + 1$. Поскольку $G_n \ge p_n > 2^{4k-1}$, а $p_s \ge p_n + 1 > 2^{4k-1} + 1$, то $N_2 < G_n$. Отсюда получаем $\sigma(G_n) > \sigma(N_2) \ge 4k\sigma(N_1)/2 = 2k\sigma(N_1)$. Следовательно $\sigma(G_n + s) = \sigma(s)\sigma(N_1) < k\frac{\sigma(G_n)}{2k} = \sigma(G_n)/2.\Box$

Обозначим $C_3(k)$ наименьшее число $n > 0$ такое, что $2^n > k$.

Лемма 3 *Если $n \ge C_3(k)$ и число s имеет не меньше $C_3(k)$ простых делителей не превосходящих p_n, то $\sigma(G_n - s, s) < \sigma(G_n, k)$.*

Доказательство. Пусть t — произведение все простых делителей s не превосходящих p_n. Тогда $G_n - s$ делится на $t \le s$. Значит выполнено неравенство $\sigma(G_n - s, s) \le \sigma(G_n - s) - \sigma(t)$. Его правая часть оценивается как $\sigma(G_n - s) - \sigma(t) < \sigma(G_n) - \sigma(t) \le \sigma(G_n) - 2^{C_3(k)} < \sigma(G_n) - k \le \sigma(G_n, k).\Box$

Обозначим $C_4(k)$ наименьшее число n при котором $p_n \ge p^3_{C_3(k)}$. Положим $C_5(k) = 3C_3(k)$.

Лемма 4 *Если $n \ge C_4(k)$, $n \ge C_5(k)$ и число $s > 0$ имеет меньше $C_3(k)$ простых делителей не превосходящих p_n, то $\sigma(G_n - s) < \sigma(G_n)/2$.*

Доказательство. Представим число $N = G_n - s$ в виде $q_1^{\beta_1}q_2^{\beta_2}\cdots q_t^{\beta_t}M$, где $q_i \le p_n$ — различные простые числа, $\beta_i > 0$, а M не имеет простых делителей меньших или равных p_n. По предположению леммы, $t < C_3(k)$. Обозначим p — наименьшее простое число, не являющееся делителем N. Поскольку $t < C_3(k) < n$, то $p \le p_{C_3(k)}$. Предположим, что $M > 1$. Тогда у M есть некоторый простой делитель p_s, $s > n$. Рассмотрим число $N_1 = p^3N/p_s$. Поскольку $p_s > p_n \ge p^3_{C_3(k)} \ge p^3$, то $N_1 < N < G_n$. Отсюда получаем $\sigma(G_n) > \sigma(N_1) \ge 4\sigma(N)/2 = 2\sigma(N)$, что и требовалось доказать.

Рассмотрим теперь случай $M = 1$. Предположим, что $q_i^{\beta_i} > p_n^4$ для некоторого i. Пусть γ_i — наименьшее число такое, что $q_i^{\gamma_i} \ge p_n$. Как мы уже показали выше, $q_i^{\gamma_i} < p_n^2$, а значит $\beta_i > 2\gamma_i$. Рассмотрим число $N_2 = p^3N/q_i^{\gamma_i} \le p_nN/p_n = N < G_n$. Отсюда получаем $\sigma(G_n) > \sigma(N_2) \ge 4\sigma(N)\frac{\beta_i-\gamma_i+1}{\beta_i+1} > \sigma(N)\frac{4\beta_i-4\gamma_i+2}{\beta_i+1} > \sigma(N)\frac{2\beta_i+2}{\beta_i+1} = 2\sigma(N)$, что и требовалось доказать. Значит $q_i^{\beta_i} \le p_n^4$ для всех i. Обозначим δ_i показатель степени q_i в расложении числа G_n на множители. Поскольку $q_i^{\delta_i} > \sqrt{p_n}$ по Лемме 1, то $\beta_i < 4\delta_i$, а значит $\beta_i + 1 < 4(\delta_i + 1)$. Получаем, что каждый простой делитель q_i может увеличить количество делителей максимум в 4 раза по сравнению с G_n. С другой стороны, каждый простой делитель не превосходящий p_n и не входящий в разложение N на множители уменьшает число делителей как минимум в 2 раза по сравнению с G_n. Учитывая эти 2 факта получаем $\sigma(N) \le 4^t\sigma(G_n)/2^{n-t} = \sigma(G_n)/2^{n-3t} \le \sigma(G_n)/2^{n-3C_3(k)+3} \le \sigma(G_n)/8 < \sigma(G_n)/2.\Box$

Доказанные леммы разбирают все нужные нам случаи. Теперь можно доказать основное утверждение.

Теорема 1 *Пусть $n \ge \max(C_1(k), C_2(k), C_4(k), C_5(k))$. Тогда $\sigma(G_n, k) > \sigma(G_n + k - s, s)$ для $0 \le s < k - 1$ и $k < s < G_n + k$.*

Доказательство. Заметим, что поскольку $\sigma(G_n) \ge 2^n \ge 2^{C_5(k)} = 2^{3C_3(k)} \ge 2^{C_3(k)+2} > 4k$, то $\sigma(G_n, k) \ge \sigma(G_n) - k > \sigma(G_n)/2$. Если $0 \le s < k - 1$, то применяя Лемму 2 получаем $\sigma(G_n + k - s, s) < \sigma(G_n + k - s) < \sigma(G_n)/2 < \sigma(G_n, k)$, что и требовалось доказать.

Если $k < s < G_n + k$, то применяя Лемму 3 в случае если у числа $s - k$ не меньше $C_3(k)$ простых делителей не превосходящих p_n получим $\sigma(G_n + k - s, s) \le \sigma(G_n - (s - k), s - k) < \sigma(G_n, k)$. В случае же если у числа $s - k$ меньше $C_3(k)$ простых делителей не превосходящих

p_n, мы получаем требуемое применяя Лемму 4: $\sigma(G_n+k-s,s) \leq \sigma(G_n-(s-k)) < \sigma(G_n)/2 < \sigma(G_n,k)$.$\square$

Из этой теоремы получаем, что число $N = G_n + k$ дает при делении на все числа от 1 до N чаще всего остаток k при условии, что $n \geq \max(C_1(k), C_2(k), C_4(k), C_5(k))$. Поскольку чисел G_n бесконечно много, отсюда следует существование требуемого числа.