

Для любого K существует n с ровно K простыми делителями, для которых $n|2^n + 1$. Поскольку если $n|2^n + 1$, где $n = q^\alpha \cdot m$, причем q - наибольший простой делитель n , то и $m|2^m + 1$. Действительно, достаточно доказать, что $m|2^n + 1 \implies m|2^m + 1$. Если положить $d = \text{ord}_m(-2)$ (m нечетно), то всякий раз, когда $m|2^\ell + 1$ для нечетного ℓ , имеем $(-2)^\ell \equiv 1 \pmod{m}$ и, следовательно, $d|\ell$. Поскольку $n|2^n + 1$, то n должно быть нечетным, но тогда $d|n$. Тем не менее, по Эйлеру-Фермату, $d|\varphi(m)$ относительно простого q^α , так как мы выбрали q больше любого простого делителя m , значит, он больше и простых делителей $\varphi(m)$. Но $\gcd(q^\alpha, d) = 1$ означает, что из $d|n$ следует $d|m$, следовательно, $(-2)^m \equiv 1 \pmod{m}$, то есть $m|2^m + 1$ (m нечетно)

Зададим $f(n) = 2^n + 1$. Заметим, что из $n|f(n)$ следует $f(n)|f(f(n))$, так как если $f(n) = n \cdot N$, то $f(f(n)) = 2^{f(n)} + 1 = (2^n)^N + 1$ делится на $2^n + 1$, поскольку N нечетно. Если $p|f(n)$, то в силу возрастания экспоненты

$$v_p(f(f(n))) = v_p((2^n)^N + 1) = v_p(2^n + 1) + v_p(N) \leq 2 \cdot v_p(f(n)) \Rightarrow \prod_{p|f(n)} p^{v_p(f(f(n)))} | f(n)^2$$

Но у нас есть $m^2 < 2^m + 1$ для целых чисел $m \geq 4$

Доказательство: Для $m = 4$, $16 = 4^2 < 2^4 + 1 = 17$. Если это верно для некоторого m , то это верно и для $(m + 1)$. Для этого заметим, что $(m + 1)^2 - 1 \leq 2(m^2 - 1)$ эквивалентно $0 \leq m^2 - 2m - 2 = (m - 1)^2 - 3$, что справедливо для $m \geq 4$, а отсюда следует, что

$$(m + 1)^2 - 1 \leq 2(m^2 - 1) < 2 \cdot 2^m = 2^{m+1} \quad \square$$

Так, если $f(n) \geq 4$, то $f(f(n))$ имеет простой делитель, который не делит $f(n)$. Но между тем он несет на себе все простые делители $f(n)$, так как $f(n)$ его делит. Поэтому в последовательности $f(3), f(f(3)), \dots$ каждый член делит следующий член (по индукции, из $3|f(3) = 9$), и каждый член не меньше 4, следовательно, по нашему предыдущему наблюдению, число простых делителей членов строго возрастает. Остается взять член, скажем, K -ый член, имеющий не менее K простых делителей, и отрезать от его факторизации наибольший простой делитель, пока не останется ровно K простых делителей