Вновь применим индукцию. База ее очевидна.

Предположим, что a_1, a_2, …, a_k – попарно взаимно простые числа. Пусть $d > 1$ – произвольный делитель числа a_{k+1}. Докажем, что d не является делителем чисел a_1, a_2, …, a_k. Рассуждая от противного, обозначим через i наименьшее число, для которого $a_i \vdots d$. Если $i > 1$, то $a_i = a_1a_2\ldots a_{i-1} + b \vdots d$ и, поскольку $b \vdots d$, произведение $a_1a_2\ldots a_{i-1}$ также делится на d, что противоречит взаимной простоте числа a_i с предшествующими членами последовательности. Если же $i = 1$, то $a_1 = a$ делится на d, что вновь приводит к противоречию (a и b – взаимно простые числа). Ⓡ

6. Обобщить конструкцию Сильвестра можно и по-другому. Пусть $a_1 = a \ge 2$, $a_{k+1} = 1 + a_k(a_k - 1)b_k$, где (b_n) – произвольная последовательность натуральных чисел. Заметим, что последовательность Сильвестра получается, если положить $a = 2$, $b_n = 1$.

Одна из задач XII Всесоюзной олимпиады в 1978 году была следующей:

Пусть $f(x) = x^3 - x + 1$, $a > 1$ – натуральное число. Докажите, что числа бесконечной последовательности a, $f(a)$, $f(f(a))$, $f(f(f(a)))$, … попарно взаимно просты.

Нетрудно видеть, что если в нашей конструкции взять $b_k = a_k + 1$, то возникнет указанная последовательность.

Докажем, что последовательность (a_n) состоит из попарно взаимно простых чисел. Действительно, если $m > k$, то

$$a_m - 1 \vdots a_{m-1} - 1 \vdots a_{m-2} - 1 \vdots \ldots \vdots a_{k+1} - 1 \vdots a_k,$$

откуда $a_m \equiv 1 \pmod{a_k}$, т.е. a_m и a_k – взаимно простые числа.[2] Ⓡ

Для дальнейшего нам понадобится следующий результат.

Лемма 2. *Пусть $k > 1$, a, b – натуральные числа. Тогда*

$$(k^a - 1, k^b - 1) = k^{(a,b)} - 1,$$

где (x, y) обозначает наибольший общий делитель чисел x и y.

Доказательство. Рассмотрим сначала случай, когда a кратно b. Тогда для некоторого q имеем $a = bq$ и $(a, b) = b$. Доказываемое равенство приобретает вид $(k^a - 1, k^b - 1) = k^b - 1$ и равносильно тому, что $k^a - 1$ кратно $k^b - 1$. Последнее утверждение легко доказать: $k^a - 1 = k^{bq} - 1 = (k^b)^q - 1$ делится на $k^b - 1$.

Пусть теперь a не делится на b, т.е. $a = bq + r$, $0 < r < b$. Имеем: $k^a - 1 = k^{bq+r} - 1 = k^r(k^{bq} - 1) + k^r - 1$. Как показано выше, $k^{bq} - 1$ делится на $k^b - 1$. Кроме того, $0 < k^r - 1 < k^b - 1$. Таким образом, остаток от деления $k^a - 1$ на $k^b - 1$ равен $k^r - 1$. Поэтому $(k^a - 1, k^b - 1) = (k^b - 1, k^r - 1)$. Используя соотношения алгоритма Евклида $a = bq_0 + r_1$, $b = r_1q_1 + r_2$, $r_1 = r_2q_2 + r_3$, …, $r_{n-2} = r_{n-1}q_{n-1} + r_n$, $r_{n-1} = q_nr_n$, получаем цепочку равенств $(k^a - 1, k^b - 1) = (k^b - 1, k^{r_1} - 1) = (k^{r_1} - 1, k^{r_2} - 1) = \ldots = (k^{r_{n-1}} - 1, k^{r_n} - 1) = k^{r_n} - 1 = k^{(a,b)} - 1$. Сопоставляя начало и конец этой цепочки, получаем требуемое.

Следствие. *Если m и n взаимно просты, то взаимно простыми будут и числа $2^m - 1$ и $2^n - 1$.*

Действительно, если $(m, n) = 1$, то $(2^m - 1, 2^n - 1) = 2^{(m,n)} - 1 = 2^1 - 1 = 1$. Ⓡ

7 (Холщинский, 1994). Предположим, что $F = \{n_1, n_2, \ldots, n_k\}$ – множество всех простых чисел ($n_1 = 2$, $n_2 = 3$, $n_3 = 5$, …). Очевидно, что числа из F попарно взаимно просты; в силу следствия леммы 2 при $i \ne j$ числа $2^{n_i} - 1$ и $2^{n_j} - 1$ также взаимно просты. Выберем теперь для каждого $i = 1, 2, \ldots, k$ какой-нибудь простой делитель p_i числа $2^{n_i} - 1$; числа p_1, p_2, …, p_k будут попарно различны. В результате образуется множество $G = \{p_1, p_2, \ldots, p_k\}$ простых чисел ($p_1 = 3$, $p_2 = 7$, $p_3 = 31$, …). Все элементы G суть нечетные числа. Поскольку множества F и G содержат поровну элементов, $2 \in F$ и $2 \notin G$, делаем вывод, что в G найдется число, не входящее в F. Пришли к противоречию. Ⓡ

Когда число имеет «много» простых делителей

Новые доказательства теоремы Евклида можно получить, строя последовательности (a_n), для которых число простых делителей n-го члена последовательности неограниченно возрастает.

8. Докажем, что число $a_n = 2^{2^n} + 2^{2^{n-1}} + 1$ имеет не менее n различных простых множителей.

В тождестве $x^4 + x^2 + 1 = (x^2 + 1 - x)(x^2 + 1 + x)$ положим $x = 2^{2^{n-1}}$. Получим

$$a_{n+1} = 2^{2^{n+1}} + 2^{2^n} + 1 =$$

$$= \left(2^{2^n} + 1 - 2^{2^{n-1}}\right)\left(2^{2^n} + 1 + 2^{2^{n-1}}\right) =$$

$$= \left(2^{2^n} + 1 - 2^{2^{n-1}}\right)a_n.$$

Таким образом, a_{n+1} делится на a_n. Числа $2^{2^n} - 2^{2^{n-1}} + 1$ и $a_n = 2^{2^n} + 2^{2^{n-1}} + 1$ взаимно просты, так как если бы у них был общий (нечетный) множитель q, то их разность $2^{2^{n-1}+1}$ делилась бы на q, что неверно. Значит, при переходе от a_n к a_{n+1} число простых делителей увеличивается. Поэтому у n-го члена рассматриваемой последовательности не менее n различных простых делителей. Ⓡ

9. Следующее доказательство возникает в результате рассмотрения представления числа $n!$ в виде произведения степеней простых чисел:

$$n! = \prod_{p \le n} p^{f_p}.$$

Как известно, кратность f_p простого числа p в каноническом разложении числа $n!$ определяется так: $f_p = \sum_{k \ge 1} \left[n/p^k\right]$. Отсюда получаем оценку для кратности f_p:

$$f_p \le \sum_k \frac{n}{p^k} = \frac{n}{p-1},$$

из которой следует, что

$$\sqrt[n]{n!} \le \prod_{p|n} p^{\frac{1}{p-1}} \qquad (2)$$

(произведение берется по всем простым делителям n). Теперь докажем неравенство

$$\sqrt[n]{n!} \ge n/e. \qquad (3)$$

Оно равносильно следующему неравенству:

$$\frac{1}{n}(\ln 2 + \ln 3 + \ldots + \ln n) \ge \ln n - 1.$$

Последнее доказывается суммированием неравенств $\ln k \ge \int_{k-1}^{k} \ln x\,dx$, где $k = 1, 2, \ldots, n$:

$$\frac{1}{n}(\ln 2 + \ln 3 + \ldots + \ln n) \ge \frac{1}{n}\int_1^n \ln x\,dx =$$

$$= \frac{1}{n}(x\ln x - x)\Big|_1^n = \frac{1}{n}(n\ln n - n + 1) =$$

$$= \ln n - 1 + \frac{1}{n} > \ln n - 1.$$

---

[2] *О сравнениях, малой теореме Ферма и функции Эйлера, которые встретятся читателю в этой статье, подробно рассказано в статье В. Сендерова и А. Спивака «Малая теорема Ферма» («Квант» №1, 3, 4 за 2000 г.).*