Сопоставив неравенства (2) и (3), получим

$$\prod_{p|n} p^{\frac{1}{p-1}} \geq \frac{n}{e}. \qquad (4)$$

Если бы множество простых чисел было конечно, то левая часть неравенства (4) не могла бы быть сколько угодно большой вопреки (4). Полученное противоречие доказывает теорему Евклида. ⟨®

10. Пусть $P(x)$ – многочлен с целыми коэффициентами. Назовем число k делителем многочлена $P(x)$, если для некоторого натурального n число $P(n)$ делится на k. Докажем, что среди делителей многочлена $P(x)$ степени ≥ 1 бесконечно много простых чисел.

Предположим, что это не так, и список простых делителей $P(x)$ исчерпывается числами $p_1, p_2, \ldots, p_s$.

Пусть $P(a) = b \neq 0$. Рассмотрим многочлен $Q(x) = P(a + bp_1p_2\ldots p_sx)/b$. Поскольку $P(a + bp_1p_2\ldots p_sx) - P(a) \vdots bp_1p_2\ldots p_s$, имеем

$$Q(x) - 1 = \frac{P(a + bp_1p_2\ldots p_sx) - P(a)}{b} \vdots bp_1p_2\ldots p_s,$$

и значит, числа $p_1, \ldots, p_s$ не являются делителями $Q(x)$. Многочлен $Q(x)$, как всякий многочлен, отличный от константы, принимает каждое свое значение конечное число раз. Поэтому среди его значений есть числа, не равные 0,1 и −1, в силу чего у него есть простые делители. Между тем всякий делитель многочлена Q является и делителем многочлена P, так как при $t = a + bp_1p_2\ldots p_sx$ выполняется равенство $P(t) = bQ(x)$.

Итак, многочлен $P(x)$ имеет простой делитель, отличный от $p_1, \ldots, p_s$. Противоречие. ⟨®

В частности, для всякой арифметической прогрессии $a_n = a_1 + (n-1)d$, где $d \neq 0$, $a \in \boldsymbol{Z}$, совокупность простых делителей ее членов бесконечна.

Знаменитая теорема Дирихле утверждает, что *если a_1 и d – взаимно простые числа, то среди членов арифметической прогрессии с первым членом a_1 и разностью d содержится бесконечно много простых чисел.*[3] В следующем разделе мы рассмотрим некоторые простейшие частные случаи этой теоремы.

[3] *Интересно отметить, что ни для одного многочлена $P(x)$ степени больше 1 не доказано, что среди чисел $P(n)$, $n \in \boldsymbol{N}$, бесконечно много простых ([2], [4]). В то же время многочлен от двух переменных $ax^2 + bxy + cy^2$, где a, b и c – взаимно простые числа, среди своих значений (при натуральных значениях аргументов) содержит бесконечно много простых чисел ([6]).*

Частные случаи теоремы Дирихле

11. *Существует бесконечно много простых чисел вида $3n + 2$.*

Пусть это не так и $p_1 = 2$, $p_2 = 5$, $p_3 = 11$, …, p_s – все простые числа указанного вида. Рассмотрим число $k = 3p_1p_2\ldots p_s - 1$. Очевидно, k не делится на 3, а также на $p_1, p_2, \ldots, p_s$. Если бы все его простые делители при делении на 3 давали остаток 1, то тем же свойством обладало бы и число k, что неверно. Значит, у числа k есть простой делитель q вида $q = 3n + 2$. Число q отлично от $p_1, \ldots, p_s$. Противоречие. ⟨®

Ясно, что если $3n + 2$ – простое число, то n нечетно. Поэтому доказанное утверждение равносильно тому, что существует бесконечно много простых чисел вида $6n + 5$. Более сложно доказывается такой факт.

12. *Существует бесконечно много простых чисел вида $6n + 1$.*

Предварительно убедимся в справедливости следующего утверждения.

Лемма 3. *Всякий простой делитель $p > 3$ многочлена $x^2 + x + 1$ имеет вид $p = 6n + 1$.*

Действительно, если $p = 3k + 2$ и $x^2 + x + 1 \vdots p$, то $x^3 \equiv 1 \pmod p$ и x не делится на p. Возведя обе части сравнения в степень k, получим $x^{p-2} \equiv 1 \pmod p$. Отсюда $x^{p-1} \equiv x \pmod p$. С другой стороны, по малой теореме Ферма $x^{p-1} \equiv 1 \pmod p$. Таким образом, $x \equiv 1 \pmod p$, $x^2 + x + 1 \equiv 3 \pmod p$ и p делится на 3. Полученное противоречие говорит о том, что простое число p при делении на 3 дает остаток 1, а значит, имеет вид $p = 6n + 1$. ⟨®

Теперь предположим, что $p_1 = 7$, $p_2 = 13$, …, p_s – все простые числа вида $6n + 1$. Пусть $m = p_1\ldots p_s$ и $k = m^2 + m + 1$. Тогда число m имеет вид $m = 6r + 1$ и $k = 36r^2 + 18r + 3 \equiv 3 \pmod 9$. Число k нечетно, не является степенью 3, поэтому у него есть простой делитель $q > 3$. По лемме 3 для некоторого n имеем $q = 6n + 1$. В то же время число q отлично от чисел $p_1, \ldots, p_s$, так как при делении k на любое число p_i в остатке будет 1. Противоречие получено. ⟨®

Рассуждения предыдущего пункта допускают обобщение.

Лемма 4. *Пусть m и p – не равные друг другу простые числа. Если p является делителем числа $x^{m-1} + x^{m-2} + \ldots + x^2 + x + 1$, где $x \in \boldsymbol{N}$, то $p \equiv 1 \pmod m$.*

Доказательство. Пусть $p = mk + r$, где $r = 1, 2, \ldots, m - 1$. Нужно доказать, что $r = 1$.

Из условия сразу следует:

$$x^m \equiv 1 \pmod p, \qquad (5)$$

т.е. число x не делится на p. Убедимся сначала, что

$$x^{r-1} \equiv 1 \pmod p. \qquad (6)$$

Если $p < m$, то $p = r$ и (6) выполняется в силу малой теоремы Ферма. Если $p > m$, то, возведя обе части сравнения (5) в степень $k = \frac{p-r}{m}$, получим

$$x^{p-r} \equiv 1 \pmod p. \qquad (7)$$

С другой стороны, по малой теореме Ферма

$$x^{p-1} \equiv 1 \pmod p. \qquad (8)$$

Вычитая из (8) сравнение (7), получаем, что $x^{p-r}\left(x^{r-1} - 1\right) \equiv 0 \pmod p$. Отсюда (поскольку x не делится на p) и следует (6).

Доказывая лемму от противного, предположим, что $r > 1$. Тогда m и $r - 1$ взаимно простые числа (так как m – простое число и $m \neq r - 1$). Применим лемму 2:

$$\left(x^m - 1, x^{r-1} - 1\right) = x^{(m,r-1)} - 1 = x - 1.$$

Из (5) и (6) следует, что число p является общим делителем чисел $x^m - 1$ и $x^{r-1} - 1$, значит, и их наибольшего общего делителя $x - 1$. Таким образом, $x \equiv 1 \pmod p$. Отсюда $P(x) \equiv m \pmod p$, и, так как по условию леммы $P(x) \equiv 0 \pmod p$, приходим к выводу: m делится на p, что противоречит условию. Значит, $r = 1$. ⟨®

13. *Существует бесконечно много простых чисел вида $mn + 1$, где m – простое число.*

Доказательство. Введем в рассмотрение многочлен

$$P(x) = x^{m-1} + x^{m-2} + \ldots + x^2 + x + 1.$$

Пусть $p_1, p_2, \ldots, p_s$ – все простые числа вида $mn + 1$. Определим число k равенством $k = P(p_1p_2\ldots p_s)$. По лемме 4 всякий простой делитель q числа k имеет вид $q = mn + 1$. В то же время число q отлично от чисел $p_1, \ldots, p_s$, так как при делении k на любое число p_i в остатке будет 1. Противоречие получено. ⟨®