Теорема (Вильсон)**.** Сравнение $(n-1)! \equiv -1 \pmod{n}$ выполнено тогда и только тогда, когда n – простое число.

Доказательство. Пусть p – простое число. Рассмотрим все числа $1, 2, 3, \ldots, p-1$. Для любого числа a в этом списке найдется такое единственное число b, что $ab \equiv 1 \pmod{p}$. (Это следует из того, что $(a, p) = 1$, поэтому можно делить 1 на a по модулю p. Остаток b будет частным.)

Итак, все числа разбиваются на пары *взаимно обратных*. Некоторые из них могли оказаться в паре сами с собой, найдем их. $a^2 \equiv 1 \pmod{p}$, значит $(a-1)(a+1) \vdots p$. Следовательно $(a+1) \vdots p$ или $(a-1) \vdots p$, то есть $a = 1$ или $a = p-1$.

Значит, все числа $2, 3, \ldots, p-2$ разбиваются уже на честные пары обратных, произведение в каждой паре дает остаток 1. Поэтому $2 \cdot 3 \cdot \ldots \cdot (p-2) \equiv 1 \pmod{p}$, а значит и $(p-1)! \equiv p-1 \equiv -1 \pmod{p}$.

Теперь в обратную сторону. Пусть n – не простое число, у него есть какой-то собственный делитель k. Но тогда в $(n-1)!$ содержится множитель k, значит $(n-1)!$ делится на k. Но -1 на k не делится, поэтому $(n-1)! \not\equiv -1 \pmod{k}$, а значит и $(n-1)! \not\equiv -1 \pmod{n}$.

Можно доказать, что для всех составных n, кроме 4, $(n-1)! \equiv 0 \pmod{n}$. □

Теорема (тождество Гаусса)**.** Пусть n – натуральное число и $d_1, d_2, \ldots, d_k$ – все его делители, включая n и само число. Тогда $\varphi(d_1) + \varphi(d_2) + \cdots + \varphi(d_k) = n$.

Доказательство. Напишем n дробей

$$\frac{0}{n}, \frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}$$

и сократим каждую из них до упора. (Дробь $\frac{0}{n}$ сокращаем до $\frac{0}{1}$.) Знаменателями новых дробей будут как раз делители d_i числа n.

Посмотрим на дроби со знаменателем d_i: $\frac{a_1}{d_i}, \frac{a_2}{d_i}, \ldots, \frac{a_s}{d_i}$. Их числители взаимно просты с d_i, потому что дроби сокращены до упора. Также все $a_j < d_i$, потому что все дроби меньше 1.

При этом любой числитель b, меньший d_i и взаимно простой с ним, у нас встретится. Действительно, если $n = kd_i$, то дробь $\frac{b}{d_i}$ получается из дроби $\frac{kb}{n}$.

Итак, дробей со знаменателем d_i столько, сколько чисел от 0 до $d_i - 1$, взаимно простых с d_i. По определению функции Эйлера, их $\varphi(d_i)$.

Дробей с каждым знаменателем по $\varphi(d_i)$, а всего их n, из этого следует желаемая формула. □