показывает, что произведение чисел, представимых в виде суммы четырех квадратов, тоже представимо в этом виде. Поэтому достаточно доказать теорему 4 для простых чисел.

Очевидно, $2 = 1^2 + 1^2 + 0^2 + 0^2$. Пусть p – нечетное простое число.

Лемма. *Существуют такие целые числа x и y, что $x^2 + y^2 + 1$ кратно p.*

Доказательство леммы. Рассмотрим числа $0^2,\ 1^2,\ 2^2,\ \ldots,\ \left(\frac{p-1}{2}\right)^2$. Если какие-то два из них дают один и тот же остаток при делении на p, т.е. если $x^2 \equiv y^2 \pmod p$, где $0 \le x < y \le (p-1)/2$, то $x^2 - y^2 = (x-y)(x+y)$ кратно p. Но ни разность $x - y$, ни сумма $x + y$ не кратна p.

Итак, рассматриваемые числа дают *разные* остатки при делении на p. Рассмотрим теперь еще $(p+1)/2$ чисел: $-1 - 0^2,\ -1 - 1^2,\ -1 - 2^2,\ \ldots$ $\ldots,\ -1 - \left(\frac{p-1}{2}\right)^2$. Они тоже дают *разные* остатки. Поскольку остатков от деления на p существует p штук, а в каждом из рассматриваемых нами множеств $(p+1)/2$ элементов, то хотя бы одно из чисел вида x^2 дает при делении на p такой же остаток, как и некоторое число вида $-1 - y^2$. При этом

$$x^2 \equiv -1 - y^2 \pmod p,$$

что и требовалось доказать:

$$x^2 + y^2 + 1 \equiv 0 \pmod p.$$

Числа x и y, как мы помним, не превосходят $(p-1)/2$; поэтому

$$x^2 + y^2 + 1 < \left(\frac{p}{2}\right)^2 + \left(\frac{p}{2}\right)^2 + 1 < p^2.$$

При этом

$$x^2 + y^2 + 1 = pm,$$

где $m < p$.

Мы хотим доказать, что число p представимо в виде суммы четырех квадратов целых чисел. Давайте рассмотрим *наименьшее* натуральное число m, для которого существуют такие целые числа $x,\ y,\ z,\ t$, что

$$x^2 + y^2 + z^2 + t^2 = pm.$$

Как мы уже знаем, $m < p$. Докажем, что $m = 1$. Для этого применим изобретенный Пьером Ферма метод бесконечного спуска: предположим, что $m > 1$, и докажем, что в таком случае m – не наименьшее.

Пусть для начала m четно. Тогда либо все числа $x,\ y,\ z,\ t$ четны, либо все они нечетны, либо два из них (для определенности, пусть это x и y) четны, а два (z и t) нечетны. В любом случае формула

$$\left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+t}{2}\right)^2 + \left(\frac{z-t}{2}\right)^2 = \frac{x^2+y^2+z^2+t^2}{2} = \frac{pm}{2}$$

показывает, что m – не наименьшее возможное.

Пусть теперь m нечетно. Рассмотрим остатки $a,\ b,\ c,\ d$ от деления чисел $x,\ y,\ z,\ t$ на m. Хотя бы один из них отличен от 0: в противном случае сумма квадратов $pm = x^2 + y^2 + z^2 + t^2$ делилась бы на m^2 и (простое!) число p делилось бы на m.

Можно считать, что числа $a,\ b,\ c,\ d$ не превосходят $(m-1)/2$. (Если, например, величина a окажется равна $(m+1)/2$ или больше, то можно заменить x на противоположное ему число $-x$. При этом вместо a получим остаток $m - a \le m - \frac{m+1}{2} = \frac{m-1}{2}$.)

Обозначим $n = a^2 + b^2 + c^2 + d^2$. Так как

$$n = a^2 + b^2 + c^2 + d^2 \equiv$$
$$\equiv x^2 + y^2 + z^2 + t^2 = pm \equiv 0 \pmod m,$$

то $n \equiv 0 \pmod m$, так что $n = ml$, где l – натуральное число. Поскольку все числа $a,\ b,\ c,\ d$ меньше $m/2$, имеем

$$ml = a^2 + b^2 + c^2 + d^2 < 4(m/2)^2 = m^2.$$

Следовательно, $l < m$.

Применим формулу Эйлера:

$$(ax+by+cz+dt)^2 + (ay-bx+ct-dz)^2 + (az-bt-cx+dy^2) + (at+bz-cy-dx)^2 =$$
$$= \left(a^2+b^2+c^2+d^2\right)\left(x^2+y^2+z^2+t^2\right) = npm = m^2pl.$$

Как мы помним, $x \equiv a,\ \ y \equiv b,\ z \equiv c$ и $t \equiv d \pmod m$. Поэтому

$$ax + by + cz + dt \equiv \equiv x^2 + y^2 + z^2 + t^2 = pm \equiv 0,$$
$$ay - bx + ct - dz \equiv \equiv xy - yx + zt - tz = 0,$$
$$az - bt - cx + dy \equiv \equiv xz - yt - zx + ty = 0,$$
$$at + bz - cy - dx \equiv \equiv xt + yz - zy - tx = 0.$$

Итак, все числа $ax + by + cz + dt$, $ay - bx + ct - dz$, $az - bt - cx + dy$ и $at + bz - cy - dx$ кратны m; формула

$$pl = \left(\frac{ax+by+cz+dt}{m}\right)^2 + \left(\frac{ay-bx+ct-dz}{m}\right)^2 + \left(\frac{az-bt-cx+dy}{m}\right)^2 + \left(\frac{at+bz-cy-dx}{m}\right)^2$$

представляет число pl в виде суммы четырех квадратов целых чисел. Таким образом, число m не является наименьшим возможным. Теорема Лагранжа доказана.

Гаусс и его теорема о семнадцатиугольнике

Подобно Архимеду Гаусс выразил желание, чтобы на его могиле был увековечен семнадцатиугольник.

Г.Вебер

Так же как в литературе Гомер, Данте, Шекспир, Гете, Толстой и Достоевский, так в математическом естествознании Архимед, Ньютон, Эйлер, Гаусс, Риман и Пуанкаре – высочайшие вершины, соединение гениальности и всеохватности.

Карл Фридрих Гаусс (1777—1855) – математик, чье имя, как и имя Архимеда, овеяно легендами. Многие его высказывания вошли в поговорку. Часто вспоминают его девиз: «Nilactum reputans si quid superesset agendum»[1]. В этой личности счастливо сплелись могучий интеллект, сильный характер и любознательность естествоиспытателя. При жиз-

[1] *Что не завершено, не сделано вовсе (лат.).*