Задача. Представить нечетное натуральное число

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

где c и d – некоторые натуральные числа разной четности

В виде произведения множителей

$$n = q_1 \times q_2$$

или доказать, что число n – простое.

Вычислить по известному n коэффициенты c и d.

Решение.

Сразу обозначим, что при перестановке c и d местами n не изменится. Действительно,

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

Поэтому, без ограничения общности, пусть c>d

Обозначим целые числа

$$a = \left(\frac{c^2 - d^2}{2} + \frac{1}{2}\right)^2 + \left(\frac{c^2 - d^2}{2} - \frac{1}{2}\right)^2 = 2\left(\frac{c^2 - d^2}{2}\right)^2 + \frac{1}{2}$$

$$b = c^2 + d^2$$

$$x = c^2 - d^2 = \left(\frac{c^2 - d^2}{2} + \frac{1}{2}\right)^2 - \left(\frac{c^2 - d^2}{2} - \frac{1}{2}\right)^2$$

Тогда, в соответствии с Пифагоровыми тройками имеем:

$$a_x^2 = a^2 - x^2 = \left(2\left(\frac{c^2 - d^2}{2} + \frac{1}{2}\right)\left(\frac{c^2 - d^2}{2} - \frac{1}{2}\right)\right)^2 = \left(2\left(\frac{c^2 - d^2}{2}\right)^2 - \frac{1}{2}\right)^2$$

$$b_x^2 = b^2 - x^2 = (2cd)^2$$

Следовательно,

$$(a^2 - x^2) - (b^2 - x^2) = a_x^2 - b_x^2 = \left(2\left(\frac{c^2 - d^2}{2} + \frac{1}{2}\right)\left(\frac{c^2 - d^2}{2} - \frac{1}{2}\right)\right)^2 - (2cd)^2$$
$$= \left(2\left(\frac{c^2 - d^2}{2} + \frac{1}{2}\right)\left(\frac{c^2 - d^2}{2} - \frac{1}{2}\right) + 2cd\right)$$
$$\times \left(2\left(\frac{c^2 - d^2}{2} + \frac{1}{2}\right)\left(\frac{c^2 - d^2}{2} - \frac{1}{2}\right) - 2cd\right)$$

Но,

$$(a^2 - x^2) - (b^2 - x^2) = a^2 - b^2 = (a+b)(a-b)$$
$$= \left(\left(\frac{c^2-d^2}{2} + \frac{1}{2}\right)^2 + \left(\frac{c^2-d^2}{2} - \frac{1}{2}\right)^2 + (c^2+d^2)\right)$$
$$\times \left(\left(\frac{c^2-d^2}{2} + \frac{1}{2}\right)^2 + \left(\frac{c^2-d^2}{2} - \frac{1}{2}\right)^2 - (c^2+d^2)\right) = 2n \times \left(2n - 2(c^2+d^2)\right)$$

Отсюда, если n – сложное, то

$$\text{НОД}(n, a_x - b_x) > 2, \text{НОД}(n, a_x + b_x) > 2$$

Действительно,

$$(a_x^2 - b_x^2) \equiv 0 (mod\ n)$$

Поскольку $a_x^2 - b_x^2 = a^2 - b^2 = 2n \times \left(2n - 2(c^2+d^2)\right)$

При этом, $a_x - b_x = 2\left(\frac{c^2-d^2}{2} + \frac{1}{2}\right)\left(\frac{c^2-d^2}{2} - \frac{1}{2}\right) - 2cd = 2\left(\frac{c^2-d^2}{2}\right)^2 - \frac{1}{2} - 2cd$

c и d разной четности, c>d, поэтому можно принять, что c=d+(2r+1), где r – натуральное. В случае, если c-d=1, то

$$a_x - b_x = 2\left(\frac{c^2-d^2}{2} + \frac{1}{2}\right)\left(\frac{c^2-d^2}{2} - \frac{1}{2}\right) - 2cd = 2\left(\frac{c+d}{2}\right)^2 - \frac{1}{2} - 2cd = 2\left(\frac{1}{2} + d\right)^2 - \frac{1}{2} - 2(1+d)d = 0$$

$$a - b = 2\left(\frac{c+d}{2}\right)^2 + \frac{1}{2} - 2cd = 2\left(\frac{c^2+2cd+d^2}{4}\right) + \frac{1}{2} - 2cd = \left(\frac{c^2-2cd+d^2}{2}\right) + \frac{1}{2}$$
$$= \frac{(c-d)^2+1}{2} = 1$$

$$a + b = 2n = 2\left(\frac{1+2d}{2}\right)^2 + \frac{1}{2} + (d+1)^2 + d^2 = 2 + 4d + 4d^2$$

$$a_x^2 - b_x^2 = a^2 - b^2$$

$$0 = 2 + 4d + 4d^2$$

Несовместное уравнение.

Подставим вместо c=d+(2r+1) в уравнение для n

$$a + b = 2 + 8\,d^2r^2 + 16\,r^3 + 4\,d + 8\,r + 16\,d\,r + 4\,d^2 + 8\,r^4 + 8\,d^2r + 16\,r^2 + 24\,d\,r^2 + 16\,d\,r^3$$

Замечаем, что по модулю 8

$$a + b \equiv 2 + 4d + 4d^2\ (mod\ 8)$$

или

$$n \equiv 1 + 2d + 2d^2 \equiv 1\ (mod\ 4)$$

Значит, n может быть только вида 4k+1, поскольку $d^2+d=d(d+1)$ -четное.

То же самое с этими формулами:

$$a_x - b_x = 2\left(\frac{c^2-d^2}{2}+\frac{1}{2}\right)\left(\frac{c^2-d^2}{2}-\frac{1}{2}\right) - 2cd = 2\left(\frac{c^2-d^2}{2}\right)^2 - \frac{1}{2} - 2cd$$
$$= 4(2\,d^2r^2 + 4\,r^3 + r + 2\,d\,r + 2\,r^4 + 2\,d^2r + 3\,r^2 + 6\,d\,r^2 + 4\,d\,r^3)$$

$$a_x + b_x = 2\left(\frac{c^2-d^2}{2}+\frac{1}{2}\right)\left(\frac{c^2-d^2}{2}-\frac{1}{2}\right) + 2cd = 2\left(\frac{c^2-d^2}{2}\right)^2 - \frac{1}{2} + 2cd$$
$$= 4(2\,d^2r^2 + 4\,r^3 + d + r + 4\,d\,r + d^2 + 2\,r^4 + 2\,d^2r + 3\,r^2 + 6\,d\,r^2 + 4\,d\,r^3)$$

Замечаем, что

$$n - (c^2 + d^2) \equiv 1 - 1 \equiv 0(mod\ 4)$$

Предположим, что n – простое. Тогда

$$a_x^2 - b_x^2 = 2n \times \left(2n - 2(c^2 + d^2)\right)$$

$$4\frac{(a_x + b_x)}{4} \times 4\frac{(a_x - b_x)}{4} = 2n \times 2 \times 4\frac{\left(n - (c^2 + d^2)\right)}{4}$$

$$\frac{(a_x + b_x)}{4} \times \frac{(a_x - b_x)}{4} = n \times \frac{\left(n - (c^2 + d^2)\right)}{4}$$

$$a_x^2 = a^2 - x^2, a_x = \sqrt{a^2 - x^2}$$

$$b_x^2 = b^2 - x^2, b_x = \sqrt{b^2 - x^2}$$

При этом

$$a_x - b_x = \sqrt{a^2 - x^2} - \sqrt{b^2 - x^2}$$

$$(a_x - b_x)^2 = a^2 + b^2 - 2x^2 - 2\sqrt{a^2 - x^2}\sqrt{b^2 - x^2} > a^2 + b^2 - 2ab$$

$$\sqrt{a^2 - x^2}\sqrt{b^2 - x^2} < ab - x^2$$

$$(a^2 - x^2)(b^2 - x^2) < a^2b^2 - 2ab\ ^2 + x^4$$

$$a^2b^2 - a^2x^2 - x^2b^2 + x^4 < a^2b^2 - 2abx^2 + x^4$$

$$-a^2 - b^2 < -2ab$$

$$0 < (a - b)^2$$

Значит,

$$2n > a - b > a_x - b_x$$

a

$$a_x + b_x = \sqrt{a^2 - x^2} + \sqrt{b^2 - x^2}$$

Следовательно,

$$a_x + b_x < a + b = 2n$$

Значит, либо $\frac{(a_x+b_x)}{4}$ должно делиться на n, либо $\frac{(a_x-b_x)}{4}$ должно делиться на n, а это невозможно, поскольку и тот, и другой множитель <n/2. Значит, n – сложное и $\frac{(a_x+b_x)}{4}$ содержит делитель n, и $\frac{(a_x-b_x)}{4}$ содержит делитель n.

Мы доказали, что

$$\text{НОД}(n, a_x - b_x) > 2, \text{НОД}(n, a_x + b_x) > 2$$

Значит,

$$q_1 = \text{НОД}(n, a_x - b_x), q_2 = \text{НОД}(n, a_x + b_x)$$

Причем, и q_1 , и q_2 обязаны содержать множители не меньше 5, поскольку n=4k+1 может содержать только множители, дающие приделении на 4 остаток 1, наименьший такой делитель и есть 5.

Попутно мы доказали, что множитель $\frac{\left(n-(c^2+d^2)\right)}{4}$ тоже не может быть простым, поскольку минимальные множители q_1 и q_2 будут содержать 5, значит, $\frac{(a_x-b_x)}{20} < \frac{(a_x+b_x)}{20} < \frac{n}{10} < \frac{\left(n-(c^2+d^2)\right)}{4}$

Причем для множителя $\frac{\left(n-(c^2+d^2)\right)}{4}$ также действуют ограничения, что c-d>1.

Соответствующие множители для $\frac{\left(n-(c^2+d^2)\right)}{4}$ будут НОД$\left(\frac{\left(n-(c^2+d^2)\right)}{4}, a_x - b_x\right)$ и НОД$\left(\frac{\left(n-(c^2+d^2)\right)}{4}, a_x + b_x\right)$

Итак, мы доказали, что при c-d>1 число n и, попутно, $\frac{\left(n-(c^2+d^2)\right)}{4}$ - сложные. Нашли множители q_1 и q_2

Теперь по известному n нужно вычислить c и d.

Сначала n умножаем на 2.

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

Наиболшее влияние оказывает сумма $\left(\frac{c^2-d^2}{2} + \frac{1}{2}\right)^2 + \left(\frac{c^2-d^2}{2} - \frac{1}{2}\right)^2$

Обозначим m=$\frac{c^2-d^2}{2} - \frac{1}{2}$. Докажем, что при увеличении m на 1 разница

$$(m+1)^2 + (m+2)^2 - (m^2 + (m+1)^2) > c^2 + d^2$$

$(m+2)^2 - m^2 > c^2 + d^2$

$m^2 + 4m + 4 - m^2 > c^2 + d^2$

$$4\left(\frac{c^2 - d^2}{2} - \frac{1}{2}\right) + 4 > c^2 + d^2$$

$2c^2 - 2d^2 - 2 + 4 > c^2 + d^2$

$c^2 - 2d^2 - 2 + 4 > d^2$

$c^2 > 3d^2 - 2$

$$c > \sqrt{3d^2 - 2}$$

При этих параметрах легко вычислить c и d по известному n.

Вычисляем $m^2 + (m+1)^2 = 2n$

$2m^2 + 2m + 1 - 2n = 0$

$$m = \frac{-2 + \sqrt{2^2 - 4 \times 2 \times (1 - 2n)}}{2 \times 2} = \frac{-1 + \sqrt{1 - 2 \times (1 - 2n)}}{2} = \frac{\sqrt{4n - 1} - 1}{2}$$

Берем целую часть:

$$m = \left[\frac{\sqrt{4n - 1} - 1}{2}\right]$$

$$\begin{cases} 2n - m^2 - (m+1)^2 = c^2 + d^2 \\ m = \dfrac{c^2 - d^2}{2} - \dfrac{1}{2} \end{cases}$$

$$\begin{cases} 2n - m^2 - (m+1)^2 = c^2 + d^2 \\ 2m = c^2 - d^2 - 1 \end{cases}$$

$$\begin{cases} 2n - m^2 - (m+1)^2 + 2m = 2c^2 - 1 \\ 2n - m^2 - (m+1)^2 - 2m = 2d^2 + 1 \end{cases}$$

$$\begin{cases} 2n - m^2 - (m+1)^2 + 2m + 1 = 2c^2 \\ 2n - m^2 - (m+1)^2 - 2m - 1 = 2d^2 \end{cases}$$

$$\begin{cases} 2n - 2m^2 = 2c^2 \\ 2n - 2(m+1)^2 = 2d^2 \end{cases}$$

$$\begin{cases} n - m^2 = c^2 \\ n - (m+1)^2 = d^2 \end{cases}$$

Использованная литература.

Только школьные учебники.