УДК 511, 514

О классе эквивалентности элементов множества примитивных пифагоровых троек

Гарипов Ильшат Ильсурович

Россия, Республика Татарстан, г. Набережные Челны
e-mail: mathsciencegaripovii@gmail.com

Аннотация

Научная статья посвящена построению и исследованию структуры классов эквивалентности элементов множества примитивных пифагоровых троек $(x; y; z)$, где $x < y$. Выведены представления примитивных пифагоровых троек $(x; y; z)$, где $z - y \leqslant 2$. Выполнено распределение этих троек по классам эквивалентности.

С помощью понятия класса эквивалентности доказана теорема о единственности существования примитивного пифагорового треугольника $(x; y; y + 1)$, описанного около окружности радиуса $r \in \mathbb{N}$. Доказаны теоремы о единственности существовании примитивной пифагоровой тройки $(x; y; y + i)$ в любых $(i = 1)$ и в конкретных $(i = 2)$ классах эквивалентности в связи с геометрией вписанных окружностей в соответствующих примитивных пифагоровых треугольниках. Получен критерий примитивно-пифагоровости тройки $(x; y; z)$, где $x < y$, разбором её составляющих.

Найдены ответы на вопросы о мощности, о структуре подмножества $[T]_{\sim,\leqslant}$ класса эквивалентности $[T]_{\sim}$.

Обосновано утверждение о непредставимости в виде полного квадрата всех составляющих любой примитивной пифагоровой тройки $(x(p); y(p); y(p) + 1)$, где p – простое число. Дана геометрическая интерпретация данного утверждения.

Выведены упрощенные геометрические формулы, связанные с вневписанными окружностями примитивного пифагорового треугольника $(x; y; y + 1)$. Проведена подготовка геометрического построения примитивного пифагорового треугольника $(x'; y'; y'+1)$ при заданном примитивном пифагоровом треугольнике $(x; y; y+1)$, описанном около окружности радиуса $r \in \mathbb{N}$. Выделены основные шаги геометрического построения такого треугольника.

Ключевые слова: примитивные пифагоровы тройки, класс эквивалентности элемента множества, простые числа, наибольший общий делитель чисел, вписанная окружность в примитивный пифагоров треугольник, вневписанные окружности примитивного пифагорового треугольника.

Перечень условных обозначений, символов

$\mathbb{N}$ – множество всех натуральных чисел.

$\mathbb{N}_0$ – множество всех неотрицательных целых чисел.

$\mathbb{N}_{2j}$ – множество всех натуральных чётных чисел.

$\mathbb{N}_{2j+1}$ – множество всех натуральных нечётных чисел.

$\mathbb{R}^+$ – множество всех положительных вещественных чисел.

$\mathbb{P}$ – множество всех простых чисел.

$\mathbb{P}^*$ – множество всех простых чисел Софи Жермен.

GCD$(x_1,...,x_n)$ – наибольший общий делитель целых чисел $x_1,..., x_n$ $(n > 1)$.

1. Введение

В научной статье речь пойдёт о примитивных пифагоровых тройках и треугольниках, о способе их генерации, о геометрическом построении таких треугольников. Будет введено понятие класса эквивалентности элемента множества Π примитивных пифагоровых троек, где первая составляющая меньше второй составляющей. Некоторые геометрические теоремы, связанные с примитивными пифагоровыми треугольниками, сформулируем и докажем в терминах класса эквивалентности. Очевидно, что многие утверждения, касающиеся множеству Π, также верны и для классов эквивалентности.

Особое внимание уделим представлениям примитивных пифагоровых троек в классах эквивалентности. Отметим, что обычная проверка (по определению) примитивно - пифагоровости тройки $(x; y; z)$ может занять много времени за счёт возведения больших составляющих данной тройки в квадрат и прямого вычисления GCD(x, y, z). Поэтому целесообразным при проверке является разбор составляющих тройки $(x; y; z)$, который заключается в следующем.

Пусть $a\%b$ обозначает остаток от деления числа $a \in \mathbb{N}$ на число $b \in \mathbb{N}$.

1) Вычисляем остатки от деления каждой составляющей тройки $(x; y; z)$ на 2. Если

$$x, y, z \in \{1; 2\} \quad \vee \quad x\%2 = y\%2 \quad \vee \quad z\%2 = 0,$$

то делаем вывод, что тройка $(x; y; z)$ не является примитивной пифагоровой.

В противном случае переходим к пункту 2).

2) Вычисляем остатки от деления каждой составляющей тройки $(x; y; z)$ на 4. Если

$$x\%4 = 2 \quad \vee \quad y\%4 = 2 \quad \vee \quad z\%4 \neq 1,$$

то делаем вывод, что тройка $(x; y; z)$ не является примитивной пифагоровой.

В противном случае переходим к пункту 3).

3) Определяем вид тройки и на основе него корректно выражаем натуральные числа k, s, h по пункту а) или б).

$$h = \frac{z-1}{4}.$$

$$\text{а) } x \in \mathbb{N}_{2j} \quad \wedge \quad y \in \mathbb{N}_{2j+1} \quad \Rightarrow \quad k = \frac{x}{4} \quad \wedge \quad s = \frac{y-q}{4}.$$

$$y\%4 = 1 \quad \Rightarrow \quad q = 1 \quad \Rightarrow \quad s = \frac{y-1}{4}.$$

$$y\%4 = 3 \quad \Rightarrow \quad q = -1 \quad \Rightarrow \quad s = \frac{y+1}{4}.$$

$$\text{б) } x \in \mathbb{N}_{2j+1} \quad \wedge \quad y \in \mathbb{N}_{2j} \quad \Rightarrow \quad s = \frac{x-q}{4} \quad \wedge \quad k = \frac{y}{4}.$$

$$x\%4 = 1 \quad \Rightarrow \quad q = 1 \quad \Rightarrow \quad s = \frac{x-1}{4}.$$

$$x\%4 = 3 \quad \Rightarrow \quad q = -1 \quad \Rightarrow \quad s = \frac{x+1}{4}.$$

3) Проверяем равенства из теоремы 2.7 относительно чисел k, s, h, q.

4) Вывод о примитивно-пифагоровости тройки $(x; y; z)$.

Особый интерес также представляет примитивная пифагорова тройка $(x; y; y+2)$, которая может и не принадлежать классу эквивалентности некоторой тройки $(x'; y'; y'+1)$. Это делает невозможным построить в объединении всех классов эквивалентности $[(x; y; y+2)]_\sim$ множество Π. В связи с этим можно ограничиться вычислением мощности и описанием структуры подмножества $[T]_{\sim,\leqslant}$ (см. стр. 13) класса эквивалентности $[T]_\sim$ через радиус окружности, вписанной в соответствующий примитивный пифагоров треугольник T.

Далее затронем тему простых чисел Софи Жермен p^* и безопасных простых чисел $2p^*+1$, которые широко применяются в криптографии с открытым ключом и при проверке числа на простоту. В рамках научной статьи эти числа находят своё отражение в примитивных пифагоровых тройках $(2p^* + 1; y; y + 1)$. В области теории чисел известна гипотеза Софи Жермен, которая гласит о бесконечности простых чисел Софи Жермен. Стоит отметить, что в каждом классе эквивалентности существует единственная тройка $T(r) = (x(r); y(r); y(r) + 1), r \in \mathbb{N}$, где $x(r) = 2r + 1$. Геометрически это будет означать, что среди примитивных пифагоровых треугольников, описанных около окружности радиуса r, найдётся единственный треугольник с меньшим катетом $x(r)$, с большим катетом $y(r)$ и с гипотенузой $z(r) = y(r)+1$. Представления этих составляющих будут даны в теореме 2.2. Возникает вопрос, возможно ли по свойствам треугольника $T(p)$, где $p \in \mathbb{P}$, сделать геометрически вывод о простоте первой составляющей $x(p)$ тройки $T(p)$. Этот вопрос в рамках научной статьи останется открытым, но будет сделан первый шаг в этом направлении, а именно будет доказано утверждение о непредставимости всех составляющих тройки $T(p)$, где $p \neq 3$, в виде полного квадрата (утверждение 4.2 и следствие 4.3).

При рассмотрении вневписанных окружностей примитивных пифагоровых треугольников $(a; b; b + 1)$ выведем упрощенные формулы:

- формулы вычисления радиуса каждой вневписанной окружности, касающейся стороны треугольника $(a;b;b+1)$ (теорема 3.1);

- формулы для попарных расстояний L между центрами вневписанных окружностей треугольника $(a;b;b+1)$ (утверждение 3.4);

- формулы для расстояний l между центром O вписанной в треугольник $(a;b;b+1)$ окружности и центром каждой из вневписанных окружностей треугольника $(a;b;b+1)$ (утверждение 3.5).

Установим связь между расстояниями L и l (вывод 3.1). Выясним, какие отрезки пропорциональны катету a треугольника $(a;b;b+1)$, радиусам r_b, r_c вневписанных окружностей треугольника $(a;b;b+1)$, не касающихся катету a (вывод 5.1). Как следствие из теоремы 3.1 получим, что если радиус вписанной в треугольник $(a;b;b+1)$ окружности есть простое число Софи Жермена p^*, то радиус r_b вневписанной окружности, касающейся стороны b треугольника $(a;b;b+1)$, выразим в виде произведения безопасного простого числа $2p^*+1$ и числа p^*.

Основываясь на полученные формулы, нарисуем вписанную, описанную и вневписанные окружности примитивного пифагорового треугольника $(a;b;b+1)$ (см. рис. 3), затем проведём подготовку (см. рис. 4) и геометрически построим примитивный пифагоров треугольник $(a';b';b'+1)$.

Перейдём теперь к самой научной статье. Сначала введём вспомогательные определения и утверждения, касающиеся к пифагоровым и примитивным пифагоровым тройкам (см. [1]).

ОПРЕДЕЛЕНИЕ 1.1. Пифагорова тройка – это упорядоченный набор $(x;y;z) \in \mathbb{N}^3$, удовлетворяющий уравнению Пифагора:

$$x^2 + y^2 = z^2. \tag{1}$$

Треугольник, длины сторон которого образуют пифагорову тройку, называется пифагоровым треугольником. Обозначим пифагоров треугольник через $(x;y;z)$, длины катетов через x, y, а длину гипотенузы через z.

Стороны треугольника $(x;y;z)$ удовлетворяют уравнению (1), и обратно, если натуральные числа x, y, z удовлетворяют уравнению (1), то треугольник со сторонами x, y, z является прямоугольным. Также отметим, что для любого пифагорового треугольника $(x;y;z)$ существует бесконечное множество ему подобных пифагоровых треугольников $(k \cdot x; k \cdot y; k \cdot z)$, $k = 1, 2, 3, \ldots$.

ТЕОРЕМА 1.1 (формула Евклида). Для любой пары $(m;n) \in \mathbb{N}^2$, где $m > n$, тройка вида $(m^2 - n^2, 2mn, m^2 + n^2)$ является пифагоровой.

ОПРЕДЕЛЕНИЕ 1.2. Пифагорова тройка $(x;y;z)$ называется примитивной, если

$$\mathrm{GCD}(x, y, z) = 1.$$

Треугольник, длины сторон которого образуют примитивную пифагорову тройку, будем называть примитивным пифагоровым треугольником.

В примитивной пифагоровой тройке $(x; y; z)$ числа x и y имеют разную чётность, причём чётное делится на 4, а z – всегда нечётно. В дальнейшем будем рассматривать только примитивные пифагоровы тройки.

ТЕОРЕМА 1.2. Любая примитивная пифагорова тройка $(x; y; z)$, где $x \in \mathbb{N}_{2j+1}$, $y \in \mathbb{N}_{2j}$; однозначно представляется в виде

$$(m^2 - n^2; 2mn; m^2 + n^2), \tag{2}$$

где $m, n \in \mathbb{N}: \ m > n,\ m - n \in \mathbb{N}_{2j+1}, \mathrm{GCD}(m, n) = 1.$

Числа m, n можно вычислить по формуле:

$$\begin{cases} m = \sqrt{\frac{z+x}{2}} = \frac{\sqrt{z+y}+\sqrt{z-y}}{2} \\ n = \sqrt{\frac{z-x}{2}} = \frac{\sqrt{z+y}-\sqrt{z-y}}{2} \end{cases}.$$

Любая такая пара чисел $(m; n)$ задаёт примитивную пифагорову тройку (2).

ОПРЕДЕЛЕНИЕ 1.3. Простое число Софи Жермен – это такое простое число p^*, что число $2p^* + 1$ также простое (см. [2]).

ОПРЕДЕЛЕНИЕ 1.4. Безопасное простое число – это простое число вида $2p^* + 1$, где p^* также простое.

ОПРЕДЕЛЕНИЕ 1.5. Отношение эквивалентности $\sim$ на множестве X – это бинарное отношение, для которого выполнены следующие условия:

1. Рефлексивность: $(\forall a \in X)(a \sim a)$.

2. Симметричность: $(\forall a, b \in X)(a \sim b \Rightarrow b \sim a)$.

3. Транзитивность: $(\forall a, b, c \in X)(a \sim b \ \wedge\ b \sim c \ \Rightarrow\ a \sim c)$.

ОПРЕДЕЛЕНИЕ 1.6. Классом эквивалентности $[a]_\sim \subset X$ элемента $a \in X$ называется подмножество элементов, эквивалентных элементу a, то есть $[a]_\sim \equiv \{x \in X | x \sim a\}$.

Любой элемент $b \in [a]_\sim$ называется представителем класса эквивалентности $[a]_\sim$.

Из определения 1.6 следует, что если $b \in [a]_\sim$, то $[a]_\sim = [b]_\sim$.

ОПРЕДЕЛЕНИЕ 1.7. Множество всех классов эквивалентности для заданного отношения эквивалентности $\sim$ на множестве X называется фактор-множеством множества X относительно $\sim$. Обозначение: $X/\sim$.

Фактор-множество $X/\sim$ является разбиением множества X.

ОПРЕДЕЛЕНИЕ 1.8. Сюръективное отображение p: $x \in X \ \mapsto\ [x]_\sim \in X/\sim$ называется естественным отображением, или канонической проекцией, множества X на фактор-множество $X/\sim$.

УТВЕРЖДЕНИЕ 1.3. Пусть X и Y – множества, $f : X \to Y$ – произвольное отображение. Тогда бинарное отношение $\sim$ на множестве X, определённое правилом:

$$(\forall x, y \in X)(x \sim y \ \Leftrightarrow \ f(x) = f(y)),$$

является отношением эквивалентности, причём существует биекция фактор-множества $X/\sim$ на множество $f(X)$ (см. [3]).

ЛЕММА 1.4. Пусть $a = bq + c$, где $a, b, c, q \in \mathbb{Z}$. Тогда

$$\text{GCD}(a, b) = \text{GCD}(b, c) \text{ (см. [4]).} \tag{3}$$

2. О классе эквивалентности элементов множества примитивных пифагоровых троек

Пусть Π – множество примитивных пифагоровых троек вида

$$\Pi \equiv \{(x; y; z) \in \mathbb{N}^3 \mid x^2 + y^2 = z^2 \ \ \wedge \ \ x < y \ \ \wedge \ \ \text{GCD}(x, y, z) = 1\}.$$

Введём функцию $f : \Pi \to \mathbb{N}$, заданную следующим образом:

$$f(x, y, z) = \tfrac{x+y-z}{2}.$$

Ясно, что функция $f(x, y, z)$ вычисляет радиус окружности, вписанной в примитивный пифагоров треугольник $(x; y; z)$. Зададим бинарное отношение $\sim$ на множестве Π по правилу:

$$(\forall \ (x; y; z), (x'; y'; z') \in \Pi)((x; y; z) \sim (x'; y'; z') \ \Leftrightarrow \ f(x, y, z) = f(x', y', z')),$$

По утверждению 1.3 отношение $\sim$ является отношением эквивалентности на множестве Π.

На основе определения 1.6 определим класс эквивалентности $[(x_1; y_1; z_1)]_\sim \subset \Pi$ элемента $(x_1; y_1; z_1) \in \Pi$:

$$[(x_1; y_1; z_1)]_\sim \equiv \{(x; y; z) \in \Pi | \ (x; y; z) \sim (x_1; y_1; z_1)\}.$$

Образуем фактор-множество $\Pi/\sim$ множества Π по заданному отношению $\sim$. Ссылаясь на утверждение 1.3, введём нумерацию классов эквивалентности в фактор-множестве $\Pi/\sim$. Номер класса эквивалентности $[(x; y; z)]_\sim$ будет соответствовать радиусу $r \in \mathbb{N}$ окружности, вписанной во все примитивные пифагоровы треугольники $(x'; y'; z') \in [(x; y; z)]_\sim$. Для удобства вместо $[(x; y; z)]_\sim$ также будем использовать запись $[(x; y; z)]_r$, где $r = f(x, y, z)$.

Перечислим некоторые элементарные свойства примитивных пифагоровых троек $(x; y; z)$.

СВОЙСТВО 2.1. В точности одна из составляющих x и y делится на 4 (см. [1]).

СВОЙСТВО 2.2. $z = 4h + 1$ при некотором $h \in \mathbb{N}$.

Справедливость данного свойства следует из теоремы о том, что все простые множители составляющей z являются простыми вида $4v + 1$ (см. [5]).

СВОЙСТВО 2.3. В точности одна из составляющих x и y делится на 3 (см. [1]).

СВОЙСТВО 2.4. Максимум одно из составляющих x, y и z является полным квадратом.

ДОКАЗАТЕЛЬСТВО. 1) В тройке $(5; 12; 13)$ все составляющие не являются полными квадратами. В тройке $(9; 40; 41)$ составляющая $x = 9$ является полным квадратом, составляющие $y = 40$, $z = 41$ не являются полным квадратом. В тройке $(3; 4; 5)$ составляющая $y = 4$ является полным квадратом, составляющие $x = 3$, $z = 5$ не являются полным квадратом. В тройке $(7; 24; 25)$ составляющая $z = 25$ является полным квадратом, составляющие $x = 7$, $y = 24$ не являются полным квадратом.

2) По теореме Ферма, нет пифагоровых треугольников, у которых хотя бы 2 стороны были квадратами (см. [1]). Следовательно, нет примитивных пифагоровых троек, у которых хотя бы 2 составляющие были квадратами. Из этого следует, что нет примитивных пифагоровых троек, у которых все составляющие были квадратами. Свойство 2.4 доказано.

Нам также понадобятся свойства наибольшего общего делителя для двух и трёх целых чисел (см. [4]).

СВОЙСТВО 2.5.

$$\mathrm{GCD}(a, b) = \mathrm{GCD}(b, a). \tag{4}$$

СВОЙСТВО 2.6.

$$\mathrm{GCD}(a, b) = \mathrm{GCD}(a, b - a). \tag{5}$$

СВОЙСТВО 2.7.

$$\mathrm{GCD}(a, b, c) = \mathrm{GCD}(\mathrm{GCD}(a, b), c) = \mathrm{GCD}(a, \mathrm{GCD}(b, c)). \tag{6}$$

СВОЙСТВО 2.8.

$$\mathrm{GCD}(2a, 2b + 1) = \mathrm{GCD}(a, 2b + 1). \tag{7}$$

СВОЙСТВО 2.9.

$$\mathrm{GCD}(2a + 1, 2b + 1) = \mathrm{GCD}(|a - b|, 2b + 1). \tag{8}$$

СВОЙСТВО 2.10.

$$\mathrm{GCD}(a, -b) = \mathrm{GCD}(a, b). \tag{9}$$

Далее разберём известную теорему, через доказательство которой выведем возможные представления всех троек из некоторого подмножества множества П.

ТЕОРЕМА 2.1. Не существует примитивных пифагоровых треугольников, у которых длины катетов равны 1 или $4k + 2$ $(k \in \mathbb{N}_0)$; и только они.

ДОКАЗАТЕЛЬСТВО. 1) Примитивные пифагоровы треугольники с чётным катетом вида $y = 4k + 2$ $(k \in \mathbb{N}_0)$ не существуют, так как y не делится на 4. Эта неделимость противоречит свойству 2.1.

Далее покажем существование примитивных пифагоровых треугольников, у которых длина катета может быть равна либо $4k$, либо $4k + 1$ $(k \in \mathbb{N})$; либо $4k + 3$ $(k \in \mathbb{N}_0)$. Для каждого случая будем использовать теорему 1.2.

2) $y = 4k$. Случай $y = 0$ (при $k = 0$) не рассматривается. Разберём случай $y \neq 0$.

$$y \in \mathbb{N}_{2j} \overset{(2)}{\Rightarrow} 4k = 2mn \Leftrightarrow 2k = mn.$$

Чтобы выполнялись $m > n, m - n \in \mathbb{N}_{2j+1}$ и GCD$(m,n) = 1$, выберем $m = 2k, n = 1$. В этом случае пара $(m; n)$ задаёт примитивную пифагорову тройку $(m^2 - n^2; 2mn; m^2 + n^2)$. Выразим эту тройку через k:

$$(m^2 - n^2; 2mn; m^2 + n^2) = (4k^2 - 1; 4k; 4k^2 + 1).$$

3) $x = 4k + 1$. Предположим, что существует примитивный пифагоров треугольник с длиной катета $x = 1$ (при $k = 0$). В этом случае из определения 1.2 следует

$$(\exists y, z \in \mathbb{N})(1 + y^2 = z^2 \quad \wedge \quad \text{GCD}(1, y, z) = 1).$$

$$1 + y^2 = z^2 \Rightarrow z = \sqrt{y^2 + 1} \notin \mathbb{N}.$$

В результате получено противоречие с натуральностью числа z. Следовательно, не существуют примитивных пифагоровых треугольников с длиной катета, равной 1.

Далее разберём случай $x \neq 1$.

$$x \in \mathbb{N}_{2j+1} \overset{(2)}{\Rightarrow} 4k + 1 = m^2 - n^2 \Leftrightarrow 4k + 1 = (m + n) \cdot (m - n).$$

$$4k + 1 = ((2k + 1) + 2k) \cdot ((2k + 1) - 2k).$$

$$(\forall k \in \mathbb{N})(2k + 1 > 2k \quad \wedge \quad (2k + 1) - 2k = 1 \in \mathbb{N}_{2j+1}) \quad \wedge$$

$$\wedge \quad (\forall k \in \mathbb{N})(\text{GCD}(2k + 1, 2k) = \text{GCD}(2k \cdot 1 + 1, 2k) \overset{(3)}{=} \text{GCD}(2k, 1) = 1) \Rightarrow$$

$$\Rightarrow (\forall k \in \mathbb{N})(2k + 1 > 2k \quad \wedge \quad (2k + 1) - 2k \in \mathbb{N}_{2j+1} \quad \wedge \quad \text{GCD}(2k + 1, 2k) = 1).$$

Тогда можно выбрать $m = 2k + 1, n = 2k$. В этом случае пара $(m; n)$ задаёт примитивную пифагорову тройку $(m^2 - n^2, 2mn, m^2 + n^2)$. Выразим эту тройку через k:

$$(m^2 - n^2; 2mn; m^2 + n^2) = (m^2 - n^2; 2mn; (m^2 - n^2) + 2n^2) =$$

$$= (4k + 1; 2 \cdot (2k + 1) \cdot (2k); 4k + 1 + 2 \cdot (2k)^2) =$$

$$= (4k + 1; 8k^2 + 4k; 8k^2 + 4k + 1).$$

4) $x = 4k + 3$ $(k \in \mathbb{N}_0)$. В этом случае,

$$x \in \mathbb{N}_{2j+1} \overset{(2)}{\Rightarrow} 4k + 3 = m^2 - n^2 \Leftrightarrow 4k + 3 = (m + n) \cdot (m - n).$$

$$4k+3=((2k+2)+(2k+1))\cdot((2k+2)-(2k+1)).$$

$$(\forall k\in\mathbb{N})(2k+2>2k+1\ \wedge\ (2k+2)-(2k+1)=1\in\mathbb{N}_{2j+1})\ \wedge$$

$$\wedge\ (\forall k\in\mathbb{N})(\text{GCD}(2k+2,2k+1)=\text{GCD}((2k+1)\cdot 1+1,2k+1)\overset{(3)}{=}\text{GCD}(2k+1,1)=1)\Rightarrow$$

$$\Rightarrow(\forall k\in\mathbb{N})(2k+2>2k+1\ \wedge\ (2k+2)-(2k+1)\in\mathbb{N}_{2j+1}\ \wedge\ \text{GCD}(2k+2,2k+1)=1).$$

Тогда можно выбрать $m=2k+2, n=2k+1$. В этом случае пара $(m;n)$ задаёт примитивную пифагорову тройку $(m^2-n^2;2mn;m^2+n^2)$. Выразим эту тройку через k:

$$(m^2-n^2;2mn;m^2+n^2)=(m^2-n^2;2mn;(m^2-n^2)+2n^2)=$$

$$=(4k+3;2\cdot(2k+2)\cdot(2k+1);4k+3+2\cdot(2k+1)^2)=$$

$$=(4k+3;8k^2+12k+4;8k^2+12k+5).$$

Теорема 2.1 доказано.

Заметим, что в случаях 3) и 4) были найдены примитивные пифагоровы тройки, в которых $x<y, z-y=1$. Найденную в случае 4) тройку приведём к следующему виду для всех $k\in\mathbb{N}$:

$$(4\cdot(k-1)+3;8\cdot(k-1)^2+12\cdot(k-1)+4;8\cdot(k-1)^2+12\cdot(k-1)+5)=$$

$$=(4k-1;8k^2-16k+8+12k-12+4;8k^2-16k+8+12k-12+5)=$$

$$=(4k-1;8k^2-4k;8k^2-4k+1).$$

В случае 2), $z-x=2$. В свою очередь,

$$4k^2-1>4k\ \Leftrightarrow\ 4k^2-4k-1>0\ \Leftrightarrow\ (2k-1)^2-2>0\ \Leftrightarrow$$

$$\Leftrightarrow\ (2k-1)^2>2\ \overset{2k-1>0}{\Leftrightarrow}\ 2k-1>\sqrt{2}\ \Leftrightarrow\ k>\tfrac{\sqrt{2}+1}{2}\ \overset{k\in\mathbb{N}}{\Leftrightarrow}\ k\geqslant 2.$$

Значит, при всех $k\geqslant 2$ верно $(4k;4k^2-1;4k^2+1)\in\Pi$.

При $k=1$ получаем примитивную пифагорову тройку $(3;4;5)\in\Pi$.

Вывод 2.1. Для всех $k\geqslant 2$ тройка вида

$$(x_{1,k};y_{1,k};z_{1,k})=(4k;4k^2-1;4k^2+1),$$

для всех $k\in\mathbb{N}$ тройки вида

$$(x_{2,k};y_{2,k};z_{2,k})=(4k+1;8k^2+4k;8k^2+4k+1),$$

$$(x_{3,k};y_{3,k};z_{3,k})=(4k-1;8k^2-4k;8k^2-4k+1)$$

являются элементами множества Π. Все эти тройки образуют множество $\Pi_{\leqslant 2}$:

$$\Pi_{\leqslant 2} \equiv \{(x; y; z) \in \Pi |\ z - y \leqslant 2\}.$$

$$f(x_{1,k}, y_{1,k}, z_{1,k}) = \tfrac{4k+4k^2-1-(4k^2+1)}{2} = \tfrac{4k-2}{2} = 2k - 1 \in \mathbb{N}_{2j+1}, k \geqslant 2.$$

$$f(x_{2,k}, y_{2,k}, z_{2,k}) = \tfrac{4k+1+8k^2+4k-(8k^2+4k+1)}{2} = \tfrac{4k}{2} = 2k \in \mathbb{N}_{2j}, k \in \mathbb{N}.$$

$$f(x_{3,k}, y_{3,k}, z_{3,k}) = \tfrac{4k-1+8k^2-4k-(8k^2-4k+1)}{2} = \tfrac{4k-2}{2} = 2k - 1 \in \mathbb{N}_{2j+1}, k \in \mathbb{N}.$$

Отсюда следует,

$$(\forall k \geqslant 2)((x_{1,k}; y_{1,k}; z_{1,k}) \notin [(x_{2,k}; y_{2,k}; z_{2,k})]_{\sim} \ \wedge \ (x_{1,k}; y_{1,k}; z_{1,k}) \in [(x_{3,k}; y_{3,k}; z_{3,k})]_{\sim}).$$

Несколько слов скажем про общее представление составляющих всех примитивных пифагоровых троек. По свойству 2.1 в точности один из катетов примитивного пифагорового треугольника $(x; y; z)$ делится на 4. Для определённости пусть x делится на 4.

$$4|x \ \Leftrightarrow \ (\exists k \in \mathbb{N})(x = 4k) \ \Rightarrow \ 4 \not| \, y \ \Rightarrow \ (\forall s \in \mathbb{N})(y \neq 4s) \ \Rightarrow$$

$$\Rightarrow \ (\exists s \in \mathbb{N})(\exists q \in \{-1; 1; 2\})(y = 4s + q).$$

С учётом теоремы 2.1 последнее равносильно утверждению

$$(\exists s \in \mathbb{N})(\exists q \in \{-1; 1\})(y = 4s + q).$$

А это равносильно утверждению

$$(\exists s \in \mathbb{N})(y = 4s - 1 \ \vee \ y = 4s + 1).$$

По свойству 2.2, $(\exists h \in \mathbb{N})(z = 4h + 1)$.

Таким образом, если в примитивном пифагоровом треугольнике $(x; y; z)$ первая составляющая x делится на 4, то $(x; y; z) = (4k; 4s + q; 4h + 1)$ при некоторых $k, s, h \in \mathbb{N}, q \in \{-1; 1\}$. Аналогично, если в примитивном пифагоровом треугольнике $(x; y; z)$ вторая составляющая y делится на 4, то $(x; y; z) = (4s + q; 4k; 4h + 1)$ при некоторых $k, s, h \in \mathbb{N}, q \in \{-1; 1\}$.

Приведём примеры:

$$(4k; 4s + q; 4h + 1) = (8; 15; 17) \ \Leftrightarrow \ k = 2, s = 4, q = -1, h = 4.$$

$$(4k; 4s + q; 4h + 1) = (20; 21; 29) \ \Leftrightarrow \ k = 5, s = 5, q = 1, h = 7.$$

$$(4s + q; 4k; 4h + 1) = (3; 4; 5) \ \Leftrightarrow \ k = 1, s = 1, q = -1, h = 1.$$

$$(4s + q; 4k; 4h + 1) = (33; 56; 65) \ \Leftrightarrow \ k = 14, s = 8, q = 1, h = 16.$$

Следующая теорема устанавливает зависимость составляющих некоторого примитивного пифагорового треугольника $(x; y; z)$ от натурального радиуса r окружности, около которой описан этот треугольник, и единственность существования такого треугольника. Краткие сообщения об этих треугольниках можно узнать в [1].

ТЕОРЕМА 2.2. Около любой окружности радиуса $r \in \mathbb{N}$ можно описать в точности один примитивный пифагоров треугольник $(x(r); y(r); z(r))$, такой, что $z(r) - y(r) = 1$. Составляющие этого треугольника выражаются через r следующим образом:

$$\begin{cases} x(r) = 2r + 1 \\ y(r) = 2r(r+1) \\ z(r) = 2r(r+1) + 1\ . \end{cases}$$

ДОКАЗАТЕЛЬСТВО. **Существование.** Пусть дана окружность радиуса $r \in \mathbb{N}$. На основе определения 1.2 построим примитивный пифагоров треугольник $(x; y; z) = (x(r); y(r); z(r))$, где $z(r) = y(r) + 1$, описанный около окружности радиуса r.

$$\text{GCD}(x, y, z) = \text{GCD}(x, y, y+1) \overset{(6)}{=} \text{GCD}(x, \text{GCD}(y, y+1)) \overset{(4)}{=}$$

$$= \text{GCD}(x, \text{GCD}(y \cdot 1 + 1, y)) \overset{(3)}{=} \text{GCD}(x, \text{GCD}(y, 1)) =$$

$$= \text{GCD}(x, 1) = 1 \;\Rightarrow\; \text{GCD}(x, y, z) = 1.$$

Ясно, что заданная окружность, вписанная в искомый треугольник $(x; y; z)$, будет иметь радиус $r = f(x, y, z)$.

$$f(x, y, z) = r \;\Leftrightarrow\; \tfrac{x+y-z}{2} = r \;\Leftrightarrow\; x + y - (y+1) = 2r \;\Leftrightarrow$$

$$\Leftrightarrow\; x - 1 = 2r \;\Leftrightarrow\; x(r) = 2r + 1.$$

$$x^2 + y^2 = z^2 \;\Leftrightarrow\; x^2 + y^2 = (y+1)^2 \;\Leftrightarrow\; x^2 + y^2 = y^2 + 2y + 1 \;\Leftrightarrow$$

$$\Leftrightarrow\; x^2 = 2y + 1 \;\Leftrightarrow\; (2r+1)^2 = 2y + 1 \;\Leftrightarrow\; 4r^2 + 4r + 1 = 2y + 1 \;\Leftrightarrow$$

$$\Leftrightarrow\; 2y = 4r^2 + 4r \;\Leftrightarrow\; y = 2r^2 + 2r \;\Leftrightarrow\; y(r) = 2r(r+1) \;\Leftrightarrow\; z(r) = 2r(r+1) + 1.$$

Таким образом, около любой окружности радиуса $r \in \mathbb{N}$ можно описать примитивный пифагоров треугольник $(2r + 1; 2r(r + 1); 2r(r + 1) + 1)$. Более того, в силу $x \not\in (y; z)$ все такие примитивные пифагоровы тройки будут элементами множества Π.

Единственность. Предположим, что около заданной окружности радиуса $r \in \mathbb{N}$ описаны $d > 1$ треугольника $(x_1; y_1; z_1), ..., (x_d; y_d; z_d) \in \Pi$, таких, что $z_i - y_i = 1, i = \overline{1; d}$.

$$\text{GCD}(x_i, y_i, z_i) = 1, i = \overline{1; d}.$$

$$(x_1; y_1; z_1) \sim ... \sim (x_d; y_d; z_d) \quad \Leftrightarrow \quad f(x_1, y_1, z_1) = ... = f(x_d, y_d, z_d).$$

$$f(x_1, y_1, z_1) = ... = f(x_d, y_d, z_d) = r \quad \Leftrightarrow \quad \tfrac{x_1+y_1-z_1}{2} = ... = \tfrac{x_d+y_d-z_d}{2} = r \quad \Leftrightarrow$$

$$\Leftrightarrow \quad x_1 + y_1 - (y_1 + 1) = ... = x_d + y_d - (y_d + 1) = 2r \quad \Leftrightarrow$$

$$\Leftrightarrow \quad x_1(r) = ... = x_d(r) = 2r + 1.$$

$$x_i^2 + y_i^2 = z_i^2,\ i = \overline{1; d} \ \Leftrightarrow \ x_i^2 + y_i^2 = (y_i + 1)^2,\ i = \overline{1; d} \ \Leftrightarrow$$

$$\Leftrightarrow \ y_1(r) = ... = y_d(r) = 2r(r + 1) \ \Leftrightarrow \ z_1(r) = ... = z_d(r) = 2r(r + 1) + 1.$$

В результате получено противоречие. Единственность установлена. Теорема 2.2 доказана.

Из теоремы 2.2 следует, что существует бесконечно много примитивных пифагоровых троек $(x; y; z) \in \Pi$, в которых $z = y + 1$.

ТЕОРЕМА 2.3. В любой треугольник можно вписать окружность и притом только одну (из построений в [6]).

Перенесём утверждения об элементах множества Π на их классы эквивалентности в $\Pi/\sim$.

УТВЕРЖДЕНИЕ 2.4. В любом классе эквивалентности $[(x; y; z)]_\sim$ элементы имеют вид либо $(4k; 4s + q; 4h + 1)$, либо $(4s + q; 4k; 4h + 1)$, где $k, s, h \in \mathbb{N}, q \in \{-1; 1\}$.

ДОКАЗАТЕЛЬСТВО. Ранее было отмечено, что все примитивные пифагоровы тройки имеют вид либо $(4k; 4s + q; 4h + 1)$, либо $(4s + q; 4k; 4h + 1)$, где $k, s, h \in \mathbb{N}, q \in \{-1; 1\}$. Отбрасывая все тройки вида $(4k; 4s + q; 4h + 1)$, где $k > s$, $(4k; 4k - 1; 4h + 1)$ и тройки вида $(4s + q; 4k; 4h + 1)$, где $s > k$, $(4k + 1; 4k; 4h + 1)$ получаем множество Π, элементы которого имеют один из видов $(4s + q; 4k; 4h + 1)$, где $s < k$, $(4k - 1; 4k; 4h + 1)$, $(4k; 4s + q; 4h + 1)$, где $k < s$, $(4k; 4k + 1; 4h + 1)$. Каждый из этих элементов может порождать класс эквивалентности, которому он принадлежит. Поэтому все указанные представления сохраняются и для элементов любого класса эквивалентности. Утверждение 2.4 доказано.

ТЕОРЕМА 2.5. В классе эквивалентности $[(x; y; z)]_\sim$ любого элемента $(x; y; z) \in \Pi$ существует единственный элемент $(x'; y'; z')$, такой, что $z' - y' = 1$.

ДОКАЗАТЕЛЬСТВО. Выберем любой элемент $(x; y; z) \in \Pi$. По определению 1.5 отношение $\sim$ удовлетворяет свойству рефлексивности. Значит, $(x; y; z) \in [(x; y; z)]_\sim$.

Из теоремы 2.3 и $(x; y; z) \in [(x; y; z)]_r$ следует, что в примитивный пифагоров треугольник $(x; y; z)$ можно вписать единственную окружность радиуса $r = f(x, y, z)$ (см. рис. 1). Из теоремы 2.2 следует, что около окружности радиуса r можно описать в точности один примитивный пифагоров треугольник $(x'; y'; z')$, такой, что $z' - y' = 1$ (см. рис. 2).

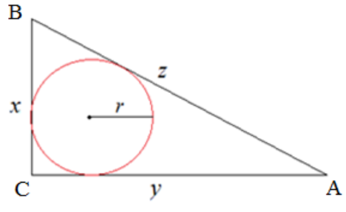


рис. 1

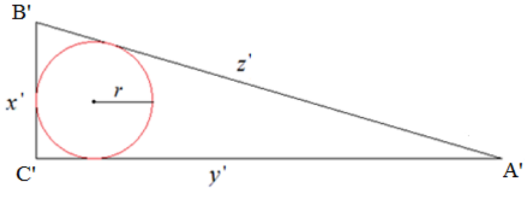


рис. 2

$$f(x', y', z') = r \;\; \wedge \;\; r = f(x, y, z) \; \Rightarrow \; f(x', y', z') = f(x, y, z) \; \Leftrightarrow$$

$$\Leftrightarrow \; (x'; y'; z') \sim (x; y; z) \; \Leftrightarrow \; (x'; y'; z') \in [(x; y; z)]_{\sim}.$$

Заметим, что если изначально принять $z = y + 1$ в примитивном пифагоровом треугольнике $(x; y; z)$, то получим $(x'; y'; z') = (x; y; z)$. Теорема 2.5 доказана.

Пусть дана окружность радиуса $r \in \mathbb{N}$. В данном случае число r – это номер некоторого класса эквивалентности $[(x'; y'; z')]_{\sim} \in \Pi/\sim$. В этом классе каждый элемент $(x; y; z)$ является примитивной пифагоровой тройкой, которая удовлетворяет равенству $r = f(x, y, z)$. Этот треугольник $(x; y; z)$ будет описан около заданной окружности.

Обратим внимание и на то, что в фактор-множестве $\Pi/\sim$ существуют классы эквивалентности $[(x'; y'; z')]_{\sim}$, в которых содержатся элементы $(x; y; z)$, где $z - y > 2$. Например,

$$[(20; 21; 29)]_6, [(28; 45; 53)]_{10}, [(33; 56; 65)]_{12}, [(36; 77; 85)]_{14}, [(48; 55; 73)]_{15}, [(39; 80; 89)]_{15}.$$

Особый интерес представляют классы эквивалентности $[(x'; y'; z')]_{\sim}$, в которых существуют элементы $(x; y; z)$, где $z - y \leqslant 2$. Построим множество $[(x'; y'; z')]_{\sim,\leqslant}$ таких элементов для любого $(x'; y'; z') \in \Pi$:

$$[(x'; y'; z')]_{\sim,\leqslant} \equiv \{(x; y; z) \in [(x'; y'; z')]_{\sim} |\; z - y \leqslant 2\}.$$

Из выше приведённого определения следует

$$(\forall (x; y; z) \in \Pi)(z - y > 2 \; \Leftrightarrow \; (x; y; z) \notin [(x; y; z)]_{\sim,\leqslant}).$$

В свою очередь, нумерация множеств $[(x'; y'; z')]_{\sim,\leqslant}$ полностью совпадает с нумерацией классов эквивалентности $[(x'; y'; z')]_{\sim}$. Очевидно, что будет верно равенство

$$\Pi_{\leqslant 2} = \bigcup_{(x;y;z) \in \Pi} [(x; y; z)]_{\sim,\leqslant}.$$

Выделим отличительное свойство в представлении элементов множества $\Pi_{\leqslant 2}$.

УТВЕРЖДЕНИЕ 2.6.

$$(\forall (x; y; z) \in \Pi_{\leqslant 2})(\forall k, s, h \in \mathbb{N})((x; y; z) \neq (4k; 4s + 1; 4h + 1)).$$

ДОКАЗАТЕЛЬСТВО. **Способ №1.** Разберём представления всех троек $(x; y; z) \in \Pi_{\leqslant 2}$ из вывода 2.1.

1) $(4k; 4k^2 - 1; 4k^2 + 1) = (4k; 4s - 1; 4h + 1)$, где $s = k^2, h = s$, для всех $k \geqslant 2$.

2) $(4k + 1; 8k^2 + 4k; 8k^2 + 4k + 1) = (4k + 1; 4k \cdot (2k + 1); 4k \cdot (2k + 1) + 1) =$

$= (4k + 1; 4s; 4h + 1)$, где $s = k \cdot (2k + 1), h = s$, для всех $k \in \mathbb{N}$.

3) $(4k-1; 8k^2-4k; 8k^2-4k+1) = (4k-1; 4k\cdot(2k-1); 4k\cdot(2k-1)+1) =$

$= (4k-1; 4s; 4h+1)$, где $s = k\cdot(2k-1), h = s$, для всех $k \in \mathbb{N}$.

Убеждаемся, что в множестве $\Pi_{\leqslant 2}$ отсутствуют тройки вида $(4k; 4s+1; 4h+1)$.

Способ №2. Докажем от противного. Предположим:

$$(\exists(x; y; z) \in \Pi_{\leqslant 2})(\exists k, s, h \in \mathbb{N})((x; y; z) = (4k; 4s+1; 4h+1)).$$

$$(x; y; z) \in \Pi_{\leqslant 2} \quad \Rightarrow \quad 0 < z - y \leqslant 2 \quad \Leftrightarrow \quad 0 < 4h + 1 - (4s+1) \leqslant 2 \quad \Leftrightarrow$$

$$\Leftrightarrow \quad 0 < 4\cdot(h-s) \leqslant 2 \quad \Leftrightarrow \quad 0 < h - s \leqslant \tfrac{1}{2}.$$

В результате получено противоречие. Утверждение 2.6 доказано.

Далее сформулируем и докажем критерий примитивно-пифагоровости заданной тройки $(x; y; z)$, где $x < y$, разбором её составляющих.

ТЕОРЕМА 2.7. Тройка $(4k; 4s+q; 4h+1)$, где $k < s$, или $(4s+q; 4k; 4h+1)$, где $s \leqslant k$, $q \in \{-1; 1\}$, является примитивной пифагоровой тогда и только тогда, когда

$$\begin{cases} k^2 + s^2 + \frac{1}{2}qs = h^2 + \frac{1}{2}h \\ \text{GCD}\left(k, |4\cdot(s-k)+q|, \left|h + (q-2)\cdot s - \frac{q-1}{2}\right|\right) = 1. \end{cases}$$

ДОКАЗАТЕЛЬСТВО. 1) Рассмотрим примитивную пифагорову тройку $(4k; 4s+q; 4h+1)$, где $k < s, q \in \{-1; 1\}$. На основании определения 1.2,

$$(4k)^2 + (4s+q)^2 = (4h+1)^2 \quad \wedge \quad \text{GCD}(4k, 4s+q, 4h+1) = 1. \tag{10}$$

$$1.1) \quad (4h+1)^2 - (4k)^2 = 16h^2 + 8h + 1 - 16k^2 = 4\cdot(4h^2 - 4k^2 + 2h) + 1 =$$

$$= 4u + 1, u = 4h^2 - 4k^2 + 2h.$$

$$(4s+q)^2 = 16s^2 + 8sq + q^2 = 16s^2 + 8sq + 1 = 4\cdot(4s^2 + 2sq) + 1 =$$

$$= 4v + 1, v = 4s^2 + 2sq.$$

$$(4k)^2 + (4s+q)^2 = (4h+1)^2 \;\Leftrightarrow\; (4s+q)^2 = (4h+1)^2 - (4k)^2 \quad \Leftrightarrow$$

$$\Leftrightarrow \quad 4v + 1 = 4u + 1 \;\Leftrightarrow\; v = u \quad \Leftrightarrow \quad 4s^2 + 2sq = 4h^2 - 4k^2 + 2h \;\Leftrightarrow$$

$$\Leftrightarrow \quad 4k^2 + 4s^2 + 2sq = 4h^2 + 2h \;\Leftrightarrow$$

$$\Leftrightarrow \quad k^2 + s^2 + \frac{1}{2}\cdot qs = h^2 + \frac{1}{2}\cdot h \; (q \in \{-1; 1\}). \tag{11}$$

$$1.2)\quad \mathrm{GCD}(4k, 4s+q, 4h+1) \overset{(6),(4)}{=} \mathrm{GCD}(\mathrm{GCD}(4k, 4h+1), 4s+q) =$$

$$= \mathrm{GCD}(\mathrm{GCD}(2\cdot(2k), 2\cdot(2h)+1), 4s+q) \overset{(7)}{=}$$

$$= \mathrm{GCD}(\mathrm{GCD}(k, 2\cdot(2h)+1), 4s+q) \overset{(6)}{=} \mathrm{GCD}(k, 4h+1, 4s+q) \;\Rightarrow$$

$$\Rightarrow\; \mathrm{GCD}(4k, 4s+q, 4h+1) = \mathrm{GCD}(k, 4h+1, 4s+q). \tag{12}$$

$$1.2.1)\;\; q=1:\;\; \mathrm{GCD}(4k, 4s+1, 4h+1) \overset{(12)}{=} \mathrm{GCD}(k, 4h+1, 4s+1) \overset{(6)}{=}$$

$$= \mathrm{GCD}(k, \mathrm{GCD}(2\cdot(2h)+1, 2\cdot(2s)+1)) \overset{(8)}{=}$$

$$= \mathrm{GCD}(k, \mathrm{GCD}(|2h-2s|, 2\cdot(2s)+1)) \overset{s\leq h}{=}$$

$$= \mathrm{GCD}(k, \mathrm{GCD}(2\cdot(h-s), 2\cdot(2s)+1)) \overset{(7)}{=}$$

$$= \mathrm{GCD}(k, \mathrm{GCD}(h-s, 2\cdot(2s)+1)) \overset{(4)}{=}$$

$$= \mathrm{GCD}(k, \mathrm{GCD}(4s+1, h-s)) \overset{(6)}{=}$$

$$= \mathrm{GCD}(\mathrm{GCD}(k, 4s+1), h-s) \overset{(5)}{=}$$

$$= \mathrm{GCD}(\mathrm{GCD}(k, 4\cdot(s-k)+1), h-s) \overset{(6)}{=}$$

$$= \mathrm{GCD}(k, 4\cdot(s-k)+1, h-s) \;\Rightarrow$$

$$\Rightarrow\; \mathrm{GCD}(4k, 4s+1, 4h+1) = \mathrm{GCD}(k, 4\cdot(s-k)+1, h-s).$$

$$1.2.2)\;\; q=-1:\;\; \mathrm{GCD}(4k, 4s-1, 4h+1) \overset{(12)}{=} \mathrm{GCD}(k, 4h+1, 4s-1) =$$

$$= \mathrm{GCD}(k, 2\cdot(2h)+1, 2\cdot(2s-1)+1) \overset{(6)}{=}$$

$$= \mathrm{GCD}(k, \mathrm{GCD}(2\cdot(2h)+1, 2\cdot(2s-1)+1)) \overset{(8)}{=}$$

$$= \mathrm{GCD}(k, \mathrm{GCD}(|2h-(2s-1)|, 2\cdot(2s-1)+1)) =$$

$$= \mathrm{GCD}(k, \mathrm{GCD}(|2\cdot(h-s)+1|, 2\cdot(2s-1)+1)) \overset{s\leq h}{=}$$

$$= \mathrm{GCD}(k, \mathrm{GCD}(2\cdot(h-s)+1, 2\cdot(2s-1)+1)) \overset{(8)}{=}$$

$$= \mathrm{GCD}(k, \mathrm{GCD}(|h-s-(2s-1)|, 2\cdot(2s-1)+1)) =$$

$$= \mathrm{GCD}(k, \mathrm{GCD}(|h-3s+1|, 4s-1)) \overset{(4)}{=}$$

$$= \mathrm{GCD}(k, \mathrm{GCD}(4s-1, |h-3s+1|)) \overset{(6)}{=}$$

$$= \text{GCD}(\text{GCD}(k, 4s-1), |h-3s+1|) \overset{(5)}{=}$$

$$= \text{GCD}(\text{GCD}(k, 4\cdot(s-k)-1), |h-3s+1|) \overset{(6)}{=}$$

$$= \text{GCD}(k, 4\cdot(s-k)-1, |h-3s+1|) \;\Rightarrow$$

$$\Rightarrow\; \text{GCD}(4k, 4s-1, 4h+1) = \text{GCD}(k, 4\cdot(s-k)-1, |h-3s+1|).$$

Из двух равенств, полученных в конце пунктов 1.2.1) и 1.2.2), построим общую формулу.

$$\text{GCD}(4k, 4s+q, 4h+1) = \text{GCD}\left(k, 4\cdot(s-k)+q, \left|h+(q-2)\cdot s-\tfrac{q-1}{2}\right|\right),\ q\in\{-1;1\}.$$

В результате условие (10) будет эквивалентно системе

$$\begin{cases} k^2+s^2+\frac{1}{2}qs = h^2+\frac{1}{2}h \\ \text{GCD}\left(k, 4\cdot(s-k)+q, \left|h+(q-2)\cdot s-\frac{q-1}{2}\right|\right)=1. \end{cases} \tag{13}$$

2) Перейдём к рассмотрению примитивной пифагоровой тройки $(4s+q; 4k; 4h+1)$, где $s\leqslant k$, $q\in\{-1;1\}$. На основании определения 1.2,

$$(4s+q)^2+(4k)^2=(4h+1)^2 \;\wedge\; \text{GCD}(4s+q, 4k, 4h+1)=1. \tag{14}$$

$$2.1)\;\; (4s+q)^2+(4k)^2=(4h+1)^2 \;\;\Leftrightarrow$$

$$\Leftrightarrow\;\; (4k)^2+(4s+q)^2=(4h+1)^2 \;\overset{(11)}{\Leftrightarrow}$$

$$\Leftrightarrow\;\; k^2+s^2+\tfrac{1}{2}qs = h^2+\tfrac{1}{2}h.$$

$$2.2)\;\; \text{GCD}(4s+q, 4k, 4h+1) \overset{(12)}{=} \text{GCD}(k, 4h+1, 4s+q).$$

2.2.1) Применим цепочку равенств из пункта 1.2.1) для выражения $\text{GCD}(4s+1, 4k, 4h+1)$.

$$q=1:\;\; \text{GCD}(4s+1, 4k, 4h+1) = \text{GCD}(k, 4h+1, 4s+1) \overset{(6),(8)}{=}$$

$$= \text{GCD}(k, \text{GCD}(|2h-2s|, 2\cdot(2s)+1)) \overset{s\leq h}{=}$$

$$= \text{GCD}(k, \text{GCD}(2\cdot(h-s), 2\cdot(2s)+1)) \overset{(4)-(7)}{=}$$

$$= \text{GCD}(\text{GCD}(k, 4\cdot(s-k)+1), h-s) \overset{s-k<0}{=}$$

$$\overset{(9)}{=} \text{GCD}(\text{GCD}(k, 4\cdot(k-s)-1), h-s) \overset{(6)}{=}$$

$$= \text{GCD}(k, 4\cdot(k-s)-1, h-s) \;\Rightarrow$$

$$\Rightarrow\ \text{GCD}(4s+1, 4k, 4h+1) = \text{GCD}(k, 4\cdot(k-s)-1, h-s).$$

2.2.2) Применим цепочку равенств из пункта 1.2.2) для выражения $\text{GCD}(4s-1, 4k, 4h+1)$.

$$q=-1:\ \text{GCD}(4s-1, 4k, 4h+1) = \text{GCD}(k, 4h+1, 4s-1) \overset{(6),(8)}{=}$$

$$= \text{GCD}(k, \text{GCD}(|2\cdot(h-s)+1|, 2\cdot(2s-1)+1)) \overset{s\leqq h}{=}$$

$$= \text{GCD}(k, \text{GCD}(2\cdot(h-s)+1, 2\cdot(2s-1)+1)) \overset{(4),(5),(6),(8)}{=}$$

$$= \text{GCD}(\text{GCD}(k, 4\cdot(s-k)-1), |h-3s+1|) \overset{s-k\leqslant 0}{=}$$

$$\overset{(9)}{=} \text{GCD}(\text{GCD}(k, 4\cdot(k-s)+1), |h-3s+1|) \overset{(6)}{=}$$

$$= \text{GCD}(k, 4\cdot(k-s)+1, |h-3s+1|) \ \Rightarrow$$

$$\Rightarrow\ \text{GCD}(4s-1, 4k, 4h+1) = \text{GCD}(k, 4\cdot(k-s)+1, |h-3s+1|).$$

Из двух равенств, полученных в конце пунктов 2.2.1) и 2.2.2), построим общую формулу.

$$\text{GCD}(4s+q, 4k, 4h+1) = \text{GCD}\left(k, 4\cdot(k-s)-q, \left|h+(q-2)\cdot s-\tfrac{q-1}{2}\right|\right),\ q\in\{-1;1\}.$$

В результате условие (14) будет эквивалентно системе

$$\begin{cases} k^2+s^2+\frac{1}{2}qs = h^2+\frac{1}{2}h \\ \text{GCD}\left(k, 4\cdot(k-s)-q, \left|h+(q-2)\cdot s-\frac{q-1}{2}\right|\right) = 1. \end{cases} \tag{15}$$

Из систем (13), (15) приходим к общей системе:

$$\begin{cases} k^2+s^2+\frac{1}{2}qs = h^2+\frac{1}{2}h \\ \text{GCD}\left(k, |4\cdot(s-k)+q|, \left|h+(q-2)\cdot s-\frac{q-1}{2}\right|\right) = 1. \end{cases}$$

Теорема 2.7 доказана.

Важный момент: полную проверку общей системы желательно сделать только при одинаковой чётности чисел s, h. Если числа s, h имеют разную чётность, то сразу делаем вывод, что рассматриваемая тройка не является примитивной пифагоровой.

Из теоремы 2.7 выводятся следующие критерии для примитивно-пифагоровости троек $(4s+q; 4h; 4h+1)$, где $q\in\{-1;1\}$, $(4k; 4h-1; 4h+1)$, где $k<h$.

Критерий №1. Тройка $(4s+q; 4h; 4h+1)$, где $q\in\{-1;1\}$, является примитивной пифагоровой тогда и только тогда, когда $s^2+\frac{1}{2}qs=\frac{1}{2}h$.

ДОКАЗАТЕЛЬСТВО. Для тройки $(4s+q; 4h; 4h+1)$ верно неравенство: $s\leqslant h$.

Данная тройка подходит под второй случай теоремы 2.7 – под тройку $(4s+q; 4k; 4h+1)$, где $k=h$. В начале доказательства теоремы 2.2 было установлено, что $\text{GCD}(x, y, y+1)=1$.

Следовательно, $\mathrm{GCD}(4s+q, 4h, 4h+1) = 1$. Исходя из этого, примитивно-пифагоровость тройки $(4s+q; 4h; 4h+1)$ эквивалентна пифагоровости этой тройки.

На основании определения 1.1, $(4s+q)^2 + (4h)^2 = (4h+1)^2$. Используем цепочку эквивалентностей из пункта 2.1) доказательства теоремы 2.7 для тройки $(4s+q; 4h; 4h+1)$.

$$(4s+q)^2 + (4h)^2 = (4h+1)^2 \;\;\Leftrightarrow\;\; h^2 + s^2 + \tfrac{1}{2}qs = h^2 + \tfrac{1}{2}h \;\;\Leftrightarrow\;\; s^2 + \tfrac{1}{2}qs = \tfrac{1}{2}h.$$

Критерий №1 доказан.

Критерий №2. Тройка $(4k; 4h-1; 4h+1)$, где $k < h$, является примитивной пифагоровой тогда и только тогда, когда $k^2 = h$.

ДОКАЗАТЕЛЬСТВО. Тройка $(4k; 4h-1; 4h+1)$ подходит под первый случай теоремы 2.7 – под тройку $(4k; 4s+q; 4h+1)$, где $s = h, q = -1$. В доказательстве теоремы 2.8 будет показано, что $\mathrm{GCD}(x, y, y+2) = 1$. Следовательно, $\mathrm{GCD}(4k, 4h-1, 4h+1) = 1$. Исходя из этого, примитивно-пифагоровость тройки $(4k; 4h-1; 4h+1)$ эквивалентна пифагоровости этой тройки.

На основании определения 1.1, $(4k)^2 + (4h-1)^2 = (4h+1)^2$. Используем цепочку эквивалентностей из пункта 1.1) доказательства теоремы 2.7 для тройки $(4k; 4h-1; 4h+1)$.

$$(4k)^2 + (4h-1)^2 = (4h+1)^2 \;\;\Leftrightarrow\;\; k^2 + h^2 + \tfrac{1}{2}\cdot(-1)\cdot h = h^2 + \tfrac{1}{2}h \;\;\Leftrightarrow\;\; k^2 = h.$$

Критерий №2 доказан.

Перейдём теперь к решению вопросу о мощности множества $[(x; y; z)]_{\sim,\leqslant}$ для каждого элемента $(x; y; z) \in \Pi$. Для этого докажем следующую теорему.

ТЕОРЕМА 2.8. В каждом классе эквивалентности $[(x'; y'; z')]_{\sim}$ имеется не более одного элемента $(x; y; z)$, такого, что $z - y = 2$.

ДОКАЗАТЕЛЬСТВО. С учётом теоремы 2.5 достаточно рассмотреть только классы эквивалентности $[(x; y; y+1)]_{\sim}$. Принимая во внимание вывод 2.1, для любой тройки $(x; y; z) \in \Pi$, где $z - y = 2$, существует класс эквивалентности $[(x'; y'; y'+1)]_{\sim}$, которому он принадлежит.

Пусть номер класса эквивалентности $[(x'; y'; y'+1)]_{\sim}$ равен r. Тогда $r = f(x', y', y'+1)$.

$$z \in \mathbb{N}_{2j+1} \;\Rightarrow\; y \in \mathbb{N}_{2j+1} \;\Rightarrow\; x \in \mathbb{N}_{2j}.$$

$$\mathrm{GCD}(x, y, z) = \mathrm{GCD}(x, y, y+2) \overset{(6)}{=} \mathrm{GCD}(x, \mathrm{GCD}(y, y+2)) \overset{(4)}{=}$$

$$= \mathrm{GCD}(x, \mathrm{GCD}(y+2, y)) = \mathrm{GCD}(x, \mathrm{GCD}(y\cdot 1 + 2, y)) \overset{(3)}{=}$$

$$= \mathrm{GCD}(x, \mathrm{GCD}(y, 2)) \overset{y\in\mathbb{N}_{2j+1}}{=} \mathrm{GCD}(x, 1) = 1 \;\Rightarrow\; \mathrm{GCD}(x, y, z) = 1.$$

$$(x; y; y+2) \in [(x'; y'; y'+1)]_{\sim} \;\Leftrightarrow\; (x; y; y+2) \sim (x'; y'; y'+1) \;\Leftrightarrow$$

$$\Leftrightarrow\; f(x, y, y+2) = f(x', y', y'+1) \;\Leftrightarrow\; f(x, y, y+2) = r \;\Leftrightarrow$$

$$\Leftrightarrow\ \tfrac{x+y-(y+2)}{2} = r\ \Leftrightarrow\ x = 2r+2.$$

$$x^2+y^2=z^2\ \Leftrightarrow\ (2r+2)^2+y^2=(y+2)^2\ \Leftrightarrow$$

$$\Leftrightarrow\ 4r^2+8r+4+y^2=y^2+4y+4\ \Leftrightarrow$$

$$\Leftrightarrow\ 4y=4r^2+8r\ \Leftrightarrow\ y=r^2+2r\ \Leftrightarrow\ z=r^2+2r+2.$$

Осталось показать, при каких $r \in \mathbb{N}$ тройка $(x;y;z)=(2r+2;r^2+2r;r^2+2r+2)$ является примитивной пифагоровой. Разберём 2 случая: $r\in\mathbb{N}_{2j}$ и $r\in\mathbb{N}_{2j+1}$.

$$1)\ r\in\mathbb{N}_{2j}\ \Rightarrow\ x=2\cdot(2j)+2=4j+2.$$

Полученное равенство противоречит теореме 2.1. Следовательно, каждый класс эквивалентности $[(x';y';y'+1)]_r$, где r – чётное, не содержит элементы вида $(x;y;y+2)$.

$$2)\ r\in\mathbb{N}_{2j+1}\ \Rightarrow$$

$$\Rightarrow\ \begin{cases} x=2\cdot(2j+1)+2=4j+4=4\cdot(j+1)=4k \\ y=(2j+1)^2+2\cdot(2j+1)=4j^2+4j+1+4j+2=4\cdot(j^2+2j+1)-1=4s-1 \\ z=(2j+1)^2+2\cdot(2j+1)+2=4h+1, \end{cases}$$

где $k=j+1, s=k^2, h=s$.

Примитивная пифагорова тройка $(x;y;z)$ приняла вид $(4k;4s-1;4h+1)$, причём имеет место неравенство $k<s$. Этот вид возможен по утверждению 2.4. Следовательно, каждый класс эквивалентности $[(x';y';y'+1)]_r$, где r – нечётное, содержит по крайней мере один элемент вида $(x;y;y+2)$.

Теперь покажем, что если такой элемент существует при нечётном r, то он единственен. Предположим, что при нечётном r существуют $d>1$ элементов $(x_i;y_i;z_i)\in[(x';y';y'+1)]_r$, таких, что $z_i=y_i+2, i=\overline{1;d}$.

$$z_i\in\mathbb{N}_{2j+1}, i=\overline{1;d}\ \ \Rightarrow\ \ y_i\in\mathbb{N}_{2j+1}, i=\overline{1;d}\ \ \Rightarrow\ \ x_i\in\mathbb{N}_{2j}, i=\overline{1;d}.$$

$$\mathrm{GCD}(x_i,y_i,z_i)=1, i=\overline{1;d}.$$

$$(x_i;y_i;z_i)\in[(x';y';y'+1)]_r, i=\overline{1;d}\ \ \Rightarrow$$

$$\Rightarrow\ (x_1;y_1;z_1)\sim\ldots\sim(x_d;y_d;z_d)\ \ \Leftrightarrow\ \ f(x_1,y_1,z_1)=\ldots=f(x_d,y_d,z_d).$$

$$f(x_1,y_1,z_1)=\ldots=f(x_d,y_d,z_d)=r\ \ \Leftrightarrow$$

$$\Leftrightarrow\ \ \tfrac{x_1+y_1-z_1}{2}=\ldots=\tfrac{x_d+y_d-z_d}{2}=r\ \ \Leftrightarrow$$

$$\Leftrightarrow \quad \tfrac{x_1+y_1-(y_1+2)}{2} = \ldots = \tfrac{x_d+y_d-(y_d+2)}{2} = r \quad \Leftrightarrow$$

$$\Leftrightarrow \quad x_1 = \ldots = x_d = 2r+2.$$

$$x_i^2 + y_i^2 = z_i^2,\, i = \overline{1;d} \quad \Leftrightarrow \quad (2r+2)^2 + y_i^2 = (y_i+2)^2,\, i = \overline{1;d} \;\Leftrightarrow$$

$$\Leftrightarrow\; y_1 = \ldots = y_d = r^2+2r \;\Leftrightarrow\; z_1 = \ldots = z_d = r^2+2r+2.$$

В результате получено противоречие. Единственность установлена.

Итак, в фактор-множестве $\Pi/\sim$ каждый класс эквивалентности содержит не более одного элемента вида $(x; y; y+2)$. Теорема 2.8 доказана.

СЛЕДСТВИЕ 2.9.

$$(\forall T \in \Pi)(|[T]_{\sim,\leqslant}| \leqslant 2).$$

Данное утверждение следует из теоремы 2.5 и теоремы 2.8.

СЛЕДСТВИЕ 2.10.

$$(\forall T \in \Pi)(f(T) \in \mathbb{N}_{2j} \;\Rightarrow\; |[T]_{\sim,\leqslant}| = 1 \;\wedge$$

$$\wedge\;(\exists k \in \mathbb{N})([T]_{\sim,\leqslant} = \{(4k+1; 4k\cdot(2k+1); 4k\cdot(2k+1)+1)\})).$$

СЛЕДСТВИЕ 2.11.

$$(\forall T \in \Pi)(f(T) \in \mathbb{N}_{2j+1} \;\Rightarrow\; |[T]_{\sim,\leqslant}| = 2 \;\wedge$$

$$\wedge\;(\exists k \in \mathbb{N})([T]_{\sim,\leqslant} = \{(4k; 4k^2-1; 4k^2+1); (4k-1; 4k\cdot(2k-1); 4k\cdot(2k-1)+1)\})).$$

Первая часть заключения следствия 2.10 и следствия 2.11 получена из доказательства теоремы 2.8 и из теоремы 2.5. Вторая часть заключения следствия 2.10 и следствия 2.11 верна в силу вывода 2.1.

Вывод 2.2.

$$(\forall T \in \Pi)(f(T) \in \mathbb{N}_{2j} \;\Rightarrow\; |[T]_{\sim,\leqslant}| = 1 \;\wedge$$

$$\wedge\;[T]_{\sim,\leqslant} = \{(2\cdot f(T)+1; 2\cdot f(T)\cdot(f(T)+1); 2\cdot f(T)\cdot(f(T)+1)+1)\}).$$

ДОКАЗАТЕЛЬСТВО. Выберем любую тройку $T \in \Pi : f(T) \in \mathbb{N}_{2j}$.

Истинность первой части заключения вывода 2.2 следует из следствия 2.10. Разберём вторую часть заключения следствия 2.10 относительно выбранной тройки:

$$(\exists k \in \mathbb{N})([T]_{\sim,\leqslant} = \{(4k+1; 4k\cdot(2k+1); 4k\cdot(2k+1)+1)\}) \quad \Leftrightarrow$$

$$\Leftrightarrow \quad (\exists k \in \mathbb{N})([T]_{\sim,\leqslant} = \{(2\cdot(2k)+1; 2\cdot(2k)\cdot(2k+1); 2\cdot(2k)\cdot(2k+1)+1)\}).$$

Из теоремы 2.2 следует, что $f(T) = 2k$ при некотором $k \in \mathbb{N}$. Тогда приведённое выше утверждение с квантором эквивалентно утверждению без кванторов:

$$[T]_{\sim,\leqslant} = \{(2 \cdot f(T) + 1; 2 \cdot f(T) \cdot (f(T) + 1); 2 \cdot f(T) \cdot (f(T) + 1) + 1)\}.$$

В результате будет получен вывод 2.2.

Вывод 2.3.

$$(\forall T \in \Pi)(f(T) \in \mathbb{N}_{2j+1} \;\Rightarrow\; |[T]_{\sim,\leqslant}| = 2 \;\wedge$$

$$\wedge\; [T]_{\sim,\leqslant} = \{(2 \cdot f(T) + 2; f(T) \cdot (f(T) + 2); f(T) \cdot (f(T) + 2) + 2)\} \cup$$

$$\cup \{(2 \cdot f(T) + 1; 2 \cdot f(T) \cdot (f(T) + 1); 2 \cdot f(T) \cdot (f(T) + 1) + 1)\}).$$

ДОКАЗАТЕЛЬСТВО. Выберем любую тройку $T \in \Pi : f(T) \in \mathbb{N}_{2j+1}$.

Истинность первой части заключения вывода 2.3 следует из следствия 2.11. Разберём вторую часть заключения следствия 2.11 относительно выбранной тройки:

$$(\exists k \in \mathbb{N})([T]_{\sim,\leqslant} = \{(4k; 4k^2 - 1; 4k^2 + 1); (4k - 1; 4k \cdot (2k - 1); 4k \cdot (2k - 1) + 1)\}).$$

Выразим все составляющие тройки $(4k - 1; 4k \cdot (2k - 1); 4k \cdot (2k - 1) + 1)$ через $2k - 1$.

$$(4k - 1; 4k \cdot (2k - 1); 4k \cdot (2k - 1) + 1) =$$

$$= (2 \cdot (2k - 1) + 1; 2 \cdot ((2k - 1) + 1) \cdot (2k - 1); 2 \cdot ((2k - 1) + 1) \cdot (2k - 1) + 1) =$$

$$= (2 \cdot (2k - 1) + 1; 2 \cdot (2k - 1) \cdot ((2k - 1) + 1); 2 \cdot (2k - 1) \cdot ((2k - 1) + 1) + 1).$$

Из теоремы 2.2 следует, что $f(T) = 2k - 1$ при некотором $k \in \mathbb{N}$.

Выразим все составляющие тройки $(4k; 4k^2 - 1; 4k^2 + 1)$ через $2k - 1$.

$$(4k; 4k^2 - 1; 4k^2 + 1) =$$

$$= (2 \cdot (2k - 1) + 2; (2k - 1) \cdot (2k + 1); (2k - 1) \cdot (2k + 1) + 2) =$$

$$= (2 \cdot (2k - 1) + 2; (2k - 1) \cdot ((2k - 1) + 2); (2k - 1) \cdot ((2k - 1) + 2) + 2).$$

Подставим $f(T)$ вместо $2k-1$ в каждом полученном выражении обеих троек, и тогда приведённое ранее утверждение с квантором будет эквивалентно утверждению без кванторов:

$$[T]_{\sim,\leqslant} = \{(2 \cdot f(T) + 2; f(T) \cdot (f(T) + 2); f(T) \cdot (f(T) + 2) + 2)\} \cup$$

$$\cup \{(2 \cdot f(T) + 1; 2 \cdot f(T) \cdot (f(T) + 1); 2 \cdot f(T) \cdot (f(T) + 1) + 1)\}.$$

В результате будет получен вывод 2.3.

3. Вневписанные окружности примитивного пифагорового треугольника $(x; y; y+1)$

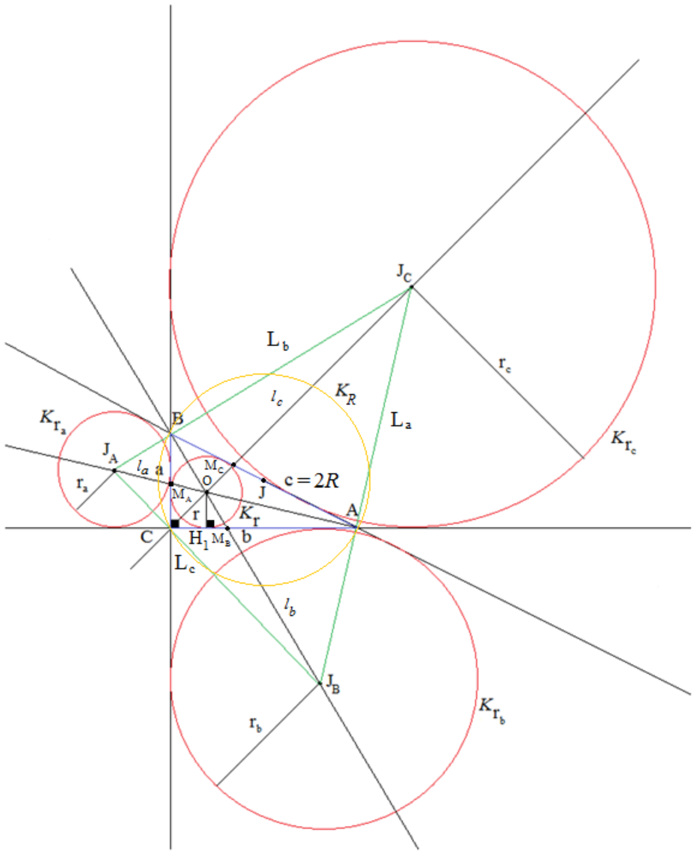


рис. 3

Рассмотрим геометрически для каждого $r \in \mathbb{N}$ элемент $T(r) = (a(r); b(r); c(r)) \in \Pi$:

$$a(r) = 2r + 1, b(r) = 2r \cdot (r+1), c(r) = 2r \cdot (r+1) + 1,$$

порождающий свой класс эквивалентности $[T(r)]_\sim$ (это следует из теоремы 2.5), то есть

$$(\forall r_1, r_2 \in \mathbb{N})(r_1 \neq r_2 \ \Rightarrow \ [T(r_1)]_\sim \cap [T(r_2)]_\sim = \varnothing).$$

Тогда будет верно равенство

$$\bigcup_{r \in \mathbb{N}} [T(r)]_\sim = \Pi.$$

В дальнейшем под $(a; b; c)$ будем понимать тройку $(a(r); b(r); c(r))$.

Для определённости пусть ΔACB – примитивный пифагоров треугольник с катетами $a \equiv BC, b \equiv AC$ и с гипотенузой $c \equiv AB$. Известно, что биссектрисы AM_A, BM_B, CM_C внутренних углов треугольника ΔACB пересекаются в одной точке O – в центре вписанной в этот треугольник окружности K_r, где r – её радиус. У треугольника ΔACB существует 3 вневписанных окружности K_{r_a}, K_{r_b}, K_{r_c}, где r_a, r_b, r_c – радиусы вневписанных окружностей с центрами J_A, J_B, J_C, касающиеся соответственно сторон a, b, c треугольника ΔACB (см. рис. 3).

Пусть R – радиус окружности K_R с центром J, описанной около треугольника ΔACB;

s – полупериметр треугольника ΔACB, то есть $s = \frac{a+b+c}{2}$.

Следующие формулы позволяют проще найти радиусы вневписанных окружностей треугольника ΔACB через r, a.

ТЕОРЕМА 3.1.

$$(\forall r \in \mathbb{N})(r_a = r + 1 \quad \wedge \quad r_b = a \cdot r \quad \wedge \quad r_c = a \cdot (r + 1)). \tag{16}$$

ДОКАЗАТЕЛЬСТВО. 1) Верна следующая формула (см. [6]):

$$(\forall r \in \mathbb{R}^+)(r \cdot r_a = (s - b) \cdot (s - c)).$$

Отсюда следует,

$$(\forall r \in \mathbb{N})(r \cdot r_a = (s - b) \cdot (s - c)).$$

$$(s - b) \cdot (s - c) = (\tfrac{a+b+c}{2} - b) \cdot (\tfrac{a+b+c}{2} - c) = (\tfrac{a-b+c}{2}) \cdot (\tfrac{a+b-c}{2}) \ \Rightarrow$$

$$\Rightarrow \ r \cdot r_a = (\tfrac{a-b+c}{2}) \cdot (\tfrac{a+b-c}{2}).$$

$$\angle C = \tfrac{\pi}{2} \ \Rightarrow \ r = \tfrac{a+b-c}{2} \ \Rightarrow \ r \cdot r_a = (\tfrac{a-b+c}{2}) \cdot r \ \Leftrightarrow \ r_a = \tfrac{a+c-b}{2}.$$

$$r_a = \tfrac{a+c-b}{2} = \tfrac{a+1}{2} = \tfrac{(2r+1)+1}{2} = \tfrac{2 \cdot (r+1)}{2} = r + 1 \ \Rightarrow \ r_a = r + 1.$$

2) Аналогично будет также верна формула (см. [6]):

$$(\forall r \in \mathbb{R}^+)(r \cdot r_b = (s - a) \cdot (s - c)).$$

Отсюда следует,

$$(\forall r \in \mathbb{N})(r \cdot r_b = (s - a) \cdot (s - c)).$$

$$(s - a) \cdot (s - c) = (\tfrac{a+b+c}{2} - a) \cdot (\tfrac{a+b+c}{2} - c) = (\tfrac{b+c-a}{2}) \cdot (\tfrac{a+b-c}{2}) \ \Rightarrow$$

$$\Rightarrow \ r \cdot r_b = (\tfrac{b+c-a}{2}) \cdot (\tfrac{a+b-c}{2}).$$

$$\angle C = \tfrac{\pi}{2} \ \Rightarrow \ r = \tfrac{a+b-c}{2} \ \Rightarrow \ r \cdot r_b = (\tfrac{b+c-a}{2}) \cdot r \ \Leftrightarrow \ r_b = \tfrac{b+c-a}{2}.$$

$$r_b = \tfrac{b+c-a}{2} = \tfrac{2r \cdot (r+1) + 2r \cdot (r+1) + 1 - (2r+1)}{2} =$$

$$= \tfrac{4r \cdot (r+1) + 1 - 2r - 1}{2} = \tfrac{4r^2 + 2r}{2} = \tfrac{2r \cdot (2r+1)}{2} = r \cdot (2r + 1) \ \Rightarrow$$

$$\Rightarrow \ r_b = a \cdot r.$$

3) По обратной теореме Фалеса, гипотенуза c будет диаметром окружности K_R. Следовательно, $c = 2R$. Далее используем известную формулу (см. [6]):

$$4R = r_a + r_b + r_c - r.$$

$$2 \cdot (2R) = (r+1) + a \cdot r + r_c - r \;\Leftrightarrow\; 2c = 1 + a \cdot r + r_c \;\Leftrightarrow$$

$$\Leftrightarrow\; 2 \cdot (2r \cdot (r+1) + 1) = 1 + (2r+1) \cdot r + r_c \;\Leftrightarrow$$

$$\Leftrightarrow\; 4r^2 + 4r + 2 = 1 + (2r+1) \cdot r + r_c \;\Leftrightarrow$$

$$\Leftrightarrow\; 4r^2 + 4r + 1 = (2r+1) \cdot r + r_c \;\Leftrightarrow$$

$$\Leftrightarrow\; (2r+1)^2 = (2r+1) \cdot r + r_c.$$

$$r_c = (2r+1)^2 - (2r+1) \cdot r = (2r+1) \cdot (2r+1-r) =$$

$$= (2r+1) \cdot (r+1) \;\Rightarrow\; r_c = a \cdot (r+1).$$

Теорема 3.1 доказана.

Из теоремы 3.1 видно, что $r_a, r_b, r_c \in \mathbb{N}$.

СЛЕДСТВИЕ 3.2.

$$(\forall p^* \in \mathbb{P}^*)(r = p^* \;\Rightarrow\; r_a = p^* + 1 \quad \wedge \quad r_b = s^* \cdot p^* \quad \wedge \quad r_c = s^* \cdot (p^* + 1)),$$

где s^* – безопасное простое число $2p^* + 1$.

СЛЕДСТВИЕ 3.3.

$$r + r_a + r_b = r_c.$$

ДОКАЗАТЕЛЬСТВО.

$$r + r_a + r_b \overset{(16)}{=} r + (r+1) + a \cdot r = (2r+1) + a \cdot r =$$

$$= a + a \cdot r = a \cdot (r+1) \overset{(16)}{=} r_c.$$

Следствие 3.3 доказано.

Из следствия 3.3 ясно, что $f(a,b,c) = r_c - (r_a + r_b)$. Используя выражения радиусов r_a, r_b из теоремы 3.1 и следствие 3.3, представим радиус любой вневписанной окружности треугольника ΔACB через радиус вписанной в треугольник ΔACB окружности и сторону, на которую касается эта вневписанная окружность:

$$r_a = a - r,\, r_b = b - r,\, r_c = c + r. \tag{17}$$

Введём обозначения для сторон треугольника $\Delta J_A J_B J_C$ (см. рис. 3):

$$L_a \equiv J_B J_C, L_b \equiv J_A J_C, L_c \equiv J_A J_B.$$

Так как в треугольнике ΔACB угол $\angle C$ – прямой, будет верно равенство

$$s = r_c.$$

Найдём формулы, которые позволяют найти попарные расстояния L_a, L_b, L_c между центрами вневписанных окружностей треугольника ΔACB, расстояния l_a, l_b, l_c между центром O окружности K_r и центром каждой из вневписанных окружностей треугольника ΔACB.

УТВЕРЖДЕНИЕ 3.4.

$$L_a = \sqrt{2} \cdot a \cdot \sqrt{c} \quad \wedge \quad L_b = (a+1) \cdot \sqrt{c} \quad \wedge \quad L_c = \sqrt{2} \cdot c.$$

ДОКАЗАТЕЛЬСТВО. За основу возьмём формулу для вычисления стороны L_a треугольника $\Delta J_A J_B J_C$ через радиус R окружности K_R и угол $\angle A$ треугольника ΔACB (см. [7]):

$$L_a = 4R \cdot \cos \tfrac{\angle A}{2}.$$

Площадь S_Δ треугольника ΔACB можно рассчитать:

– через R и все стороны треугольника ΔACB:

$$S_\Delta = \tfrac{abc}{4R}.$$

– через все стороны и полупериметр s треугольника ΔACB с помощью формулы Герона (см. [6]):

$$S_\Delta = \sqrt{s(s-a)(s-b)(s-c)}.$$

$$\frac{abc}{4R} = \sqrt{s(s-a)(s-b)(s-c)} \quad \Leftrightarrow \quad R = \frac{abc}{4 \cdot \sqrt{s(s-a)(s-b)(s-c)}}. \tag{18}$$

Далее используем формулу для нахождения $\cos \frac{\angle A}{2}$ через все стороны и полупериметр s треугольника ΔACB (см. [8]):

$$\cos \tfrac{\angle A}{2} = \sqrt{\tfrac{s(s-a)}{bc}}.$$

$$L_a \overset{(18)}{=} 4 \cdot \tfrac{abc}{4 \cdot \sqrt{s(s-a)(s-b)(s-c)}} \cdot \sqrt{\tfrac{s(s-a)}{bc}} = \tfrac{a}{\sqrt{(s-b)(s-c)}} \cdot \tfrac{bc}{\sqrt{bc}} = a \cdot \sqrt{\tfrac{bc}{(s-b)(s-c)}}.$$

Стороны L_b, L_c треугольника $\Delta J_A J_B J_C$ находятся аналогично. Таким образом,

$$L_a = a \cdot \sqrt{\tfrac{b \cdot c}{(s-b)(s-c)}} \quad \wedge \quad L_b = b \cdot \sqrt{\tfrac{a \cdot c}{(s-a)(s-c)}} \quad \wedge \quad L_c = c \cdot \sqrt{\tfrac{a \cdot b}{(s-a)(s-b)}}.$$

Из доказательства теоремы 3.1 вытекают следующие равенства:

$$s - a = r_b \overset{(16)}{=} a \cdot r \quad \wedge \quad s - b = r_a \overset{(16)}{=} r + 1 \quad \wedge \quad s - c = r. \tag{19}$$

$$L_a \overset{(19)}{=} a \cdot \sqrt{\frac{2r\cdot(r+1)\cdot c}{(r+1)\cdot r}} = \sqrt{2} \cdot a \cdot \sqrt{c}.$$

$$L_b \overset{(19)}{=} b \cdot \sqrt{\frac{a\cdot c}{(a\cdot r)\cdot r}} = b \cdot \sqrt{\frac{c}{r^2}} = \frac{2r\cdot(r+1)}{r} \cdot \sqrt{c} =$$

$$= 2 \cdot (r+1) \cdot \sqrt{c} = ((2r+1)+1) \cdot \sqrt{c} = (a+1) \cdot \sqrt{c}.$$

$$L_c \overset{(19)}{=} c \cdot \sqrt{\frac{a\cdot 2r\cdot(r+1)}{(a\cdot r)\cdot(r+1)}} = \sqrt{2} \cdot c.$$

Утверждение 3.4 доказано.

Подчеркнём, что $\Delta J_A J_B J_C$ является треугольником трёх внешних биссектрис. Тогда треугольник ΔACB является ортотреугольником для треугольника $\Delta J_A J_B J_C$. Следовательно, в треугольнике $\Delta J_A J_B J_C$ отрезки $J_C C, J_B B, J_A A$ являются высотами.

Введём обозначения: $l_a \equiv OJ_A$, $l_b \equiv OJ_B$, $l_c \equiv OJ_C$.

УТВЕРЖДЕНИЕ 3.5.

$$l_a = \sqrt{2} \cdot \sqrt{c} \quad \wedge \quad l_b = (a-1) \cdot \sqrt{c} \quad \wedge \quad l_c = \sqrt{2} \cdot c.$$

ДОКАЗАТЕЛЬСТВО. Рассмотрим прямоугольный треугольник AH_1O (см. рис. 3). Так как AO – отрезок биссектрисы AM_A угла $\angle A$ треугольника ΔACB, будет верно равенство

$$\angle OAH_1 = \frac{\angle A}{2}.$$

В свою очередь, $\sin \angle OAH_1 = \frac{r}{AO}$. Следовательно, $\sin \frac{\angle A}{2} = \frac{r}{AO}$.

Справедливо следующее соотношение (см. [7]):

$$AO \cdot l_a = 4Rr. \tag{20}$$

Выразим l_a через радиус R окружности K_R и угол $\angle A$ треугольника ΔACB.

$$l_a = 4R \cdot \left(\frac{r}{AO}\right) = 4R \cdot \sin \frac{\angle A}{2}.$$

Далее используем формулу для нахождения $\sin \frac{\angle A}{2}$ через стороны b, c и полупериметр s треугольника ΔACB (см. [8]):

$$\sin \frac{\angle A}{2} = \sqrt{\frac{(s-b)(s-c)}{bc}}.$$

$$l_a \overset{(18)}{=} 4 \cdot \frac{abc}{4\cdot\sqrt{s(s-a)(s-b)(s-c)}} \cdot \sqrt{\frac{(s-b)(s-c)}{bc}} = \frac{a}{\sqrt{s(s-a)}} \cdot \frac{bc}{\sqrt{bc}} = a \cdot \sqrt{\frac{bc}{s(s-a)}}.$$

Расстояния l_b, l_c находятся аналогично. Таким образом,

$$l_a = a \cdot \sqrt{\frac{bc}{s(s-a)}} \quad \wedge \quad l_b = b \cdot \sqrt{\frac{a\cdot c}{s\cdot(s-b)}} \quad \wedge \quad l_c = c \cdot \sqrt{\frac{a\cdot b}{s\cdot(s-c)}}.$$

$$l_a \overset{(19)}{=} a \cdot \sqrt{\frac{2r\cdot(r+1)\cdot c}{a\cdot(r+1)\cdot(a\cdot r)}} = a \cdot \sqrt{\frac{2r\cdot(r+1)\cdot c}{a^2\cdot r\cdot(r+1)}} = \sqrt{2} \cdot \sqrt{c}.$$

$$l_b \overset{(19)}{=} 2r \cdot (r+1) \cdot \sqrt{\tfrac{a \cdot c}{a \cdot (r+1) \cdot (r+1)}} = 2r \cdot \sqrt{c} =$$

$$= ((2r+1) - 1) \cdot \sqrt{c} = (a-1) \cdot \sqrt{c}.$$

$$l_c \overset{(19)}{=} c \cdot \sqrt{\tfrac{a \cdot (2r \cdot (r+1))}{a \cdot (r+1) \cdot r}} = \sqrt{2} \cdot c.$$

Утверждение 3.5 доказано.

Найдём расстояния l_a, l_b, l_c через стороны треугольника ΔACB и расстояния L_a, L_b, L_c соответственно.

Вывод 3.1.

$$l_a = \tfrac{L_a}{a} \quad \wedge \quad l_b = L_b - 2 \cdot \sqrt{b+1} \quad \wedge \quad l_c = L_c.$$

ДОКАЗАТЕЛЬСТВО. Выше приведённые равенства получаются применением равенств в утверждениях 3.4, 3.5.

$$l_a = \sqrt{2} \cdot \sqrt{c} = \tfrac{\sqrt{2} \cdot a \cdot \sqrt{c}}{a} = \tfrac{L_a}{a}.$$

$$l_b = (a-1) \cdot \sqrt{c} = (a+1-2) \cdot \sqrt{c} =$$

$$= (a+1) \cdot \sqrt{c} - 2 \cdot \sqrt{c} = L_b - 2 \cdot \sqrt{b+1}.$$

$$l_c = \sqrt{2} \cdot c = L_c.$$

Вывод 3.1 получен.

4. Простые числа в составляющих примитивной пифагоровой тройки $(x; y; y+1)$

Для каждого $p \in \mathbb{P}$ выберем элемент $T(p) \in \Pi$:

$$T(p) = (2p+1; 2p \cdot (p+1); 2p \cdot (p+1) + 1),$$

порождающий свой класс эквивалентности $[T(p)]_{\sim}$. Полученное множество таких элементов обозначим через F:

$$F \equiv \bigcup_{p \in \mathbb{P}} \{T(p)\}.$$

Множество F счётно в силу счётности множества P всех простых чисел.

Теперь сформулируем необходимое условие для того, чтобы заданное целое число, большее 3, было простым числом Софи Жермена.

УТВЕРЖДЕНИЕ 4.1. Если $p > 3$ является простым числом Софи Жермен, то

$$p \equiv 2 \ (\mathrm{mod}\ 3).$$

Выясним, какие представления будут подходящими для числа $p \in \mathbb{P}$ и первой составляющей $2p+1 \in \mathbb{P}$ элемента $T(p)$ множества F.

1) $p = 3t \notin \mathbb{P}$ при любом $t \in \mathbb{N} \setminus \{1\}$. Случай 1) отпадает.

Число $p = 3$ является простым числом Софи Жермена, так как $2p+1 = 7 \in \mathbb{P}$.

2) $p = 3t+1$ $(t \in \mathbb{N})$. Случай 2) отпадает в силу утверждения 4.1.

3) $p = 3t+2$ $(t \in \mathbb{N})$:

$$\text{а) } t = 2j, j \in \mathbb{N} \;\Rightarrow\; p = 3\cdot(2j)+2 = 2\cdot(3j)+2 = 2\cdot(3j+1) \notin \mathbb{P}, j \in \mathbb{N}.$$

Случай 3) а) отпадает.

Число $p = 2$ является простым числом Софи Жермена, так как $2p+1 = 5 \in \mathbb{P}$.

Обозначим дополнение множества $\mathbb{P}$ до множества $\mathbb{N}$ через $\overline{\mathbb{P}}$.

$$\text{б) } t = 2j+1, j \in \mathbb{N}_0 \;\Rightarrow\; p = 3\cdot(2j+1)+2 = 6\cdot(j+1)-1 \in \mathbb{P}\cup\overline{\mathbb{P}}, j \in \mathbb{N}_0 \;\Rightarrow$$

$$\Rightarrow\; p = 6v-1 \in \mathbb{P}\cup\overline{\mathbb{P}}, v \in \mathbb{N} \;\Rightarrow\; 2p+1 = 2\cdot(6v-1)+1 = 12v-1 \in \mathbb{P}\cup\overline{\mathbb{P}}, v \in \mathbb{N}.$$

В итоге, подходящими являются пары чисел:

$$1)\ p = 2 \in \mathbb{P}, 2p+1 = 5 \in \mathbb{P}.$$

$$2)\ p = 3 \in \mathbb{P}, 2p+1 = 7 \in \mathbb{P}.$$

$$3)\ p = 6v-1 \in \mathbb{P}, 2p+1 = 12v-1 \in \mathbb{P} \text{ при некоторых } v \in \mathbb{N}.$$

Генерируя все выше указанные безопасные простые числа $2p+1$, можно построить множество $F^* \subset F$ всех троек, в которых первая составляющая есть безопасное простое число. Первая составляющая $2p^*+1$ любой тройки $T(p^*) \in F^*$ $(p^* \in P^*)$ не делится на 3. Тогда по свойству 2.3 вторая составляющая $2p^*(p^*+1)$ тройки $T(p^*)$ делится на 3. Заметим, что утверждение о делимости на 3 второй составляющей тройки $T(p)$ для множества F не всегда будет верным. Например, $(15; 112; 113)$ при $p = 7$; $(27; 364; 365)$ при $p = 13$.

Проблема генерации безопасных простых чисел тесно связана со следующей гипотезой.

ГИПОТЕЗА 4.1 (гипотеза Софи Жермен). Множество P^* бесконечно.

Следовательно, задачу о бесконечности множества P^* можно свести к задаче о бесконечности множества F^*. Важно отметить, что $|F^*| = |P^*|$.

Дальше речь пойдёт о непредставимости в виде полного квадрата всех составляющих троек из множества F.

УТВЕРЖДЕНИЕ 4.2. Для любого простого числа $p \neq 3$ все составляющие элементов $T(p)$ множества F не являются полными квадратами.

ДОКАЗАТЕЛЬСТВО. Учитывая свойство 2.4, рассмотрим 3 случая относительно составляющих любого элемента $T(p)$ множества F.

1) Предположим: $(\exists p \in \mathbb{P})(\exists a \in \mathbb{N})(2p+1 = a^2)$. Для всех $a \in \mathbb{N}_{2j}$ равенство не выполняется. Тогда равенство должно выполняться для некоторого $a \in \mathbb{N}_{2j+1}$.

$$a = 2j + 1 \;\Rightarrow\; 2p + 1 = (2j+1)^2 \;\Leftrightarrow$$

$$\Leftrightarrow\; 2p + 1 = 4j^2 + 4j + 1 \;\Rightarrow\; p = 2 \cdot (j^2 + j) \notin \mathbb{P}.$$

Получено противоречие с простотой числа p. В таком случае будет верно утверждение:

$$(\forall p \in \mathbb{P})(\forall a \in \mathbb{N})(2p + 1 \neq a^2).$$

2) Предположим: $(\exists p \in \mathbb{P})(\exists a \in \mathbb{N})(2p \cdot (p+1) = a^2)$. Для всех $a \in \mathbb{N}_{2j+1}$ равенство не выполняется. Тогда равенство должно выполняться для некоторого $a \in \mathbb{N}_{2j}$.

$$a = 2j \;\Rightarrow\; 2p \cdot (p+1) = (2j)^2 \;\Leftrightarrow$$

$$\Leftrightarrow\; 2p \cdot (p+1) = 4j^2 \;\Leftrightarrow\; p \cdot (p+1) = 2j^2.$$

а) $p = 2$. Тогда $j^2 = 3$. Следовательно, $j = \sqrt{3}$ не является натуральным числом.
Получено противоречие с натуральностью числа j.
б) $p \neq 2$. Тогда $p + 1$ делится на 2.

$$p \cdot (p+1) = 2j^2 \;\Leftrightarrow\; p \cdot \left(\tfrac{p+1}{2}\right) = j^2 \;\Rightarrow\; p \mid \tfrac{p+1}{2}.$$

$$\tfrac{p+1}{2} < p \;\Rightarrow\; p \nmid \tfrac{p+1}{2}.$$

Получено противоречие. В таком случае будет верно утверждение:

$$(\forall p \in \mathbb{P})(\forall a \in \mathbb{N})(2p \cdot (p+1) \neq a^2).$$

3) Верно: $(\exists!\ p \in \mathbb{P})(\exists!\ a \in \mathbb{N})(2p(p+1) + 1 = a^2)$. Покажем это.

Для всех $a \in \mathbb{N}_{2j}$ равенство не выполняется. Тогда равенство должно выполняться для некоторого $a \in \mathbb{N}_{2j+1}$.

$$2p(p+1) + 1 = a^2 \;\Leftrightarrow\; 2p^2 + 2p + 1 = a^2 \;\Leftrightarrow$$

$$\Leftrightarrow\; p^2 + (p^2 + 2p + 1) = a^2 \;\Leftrightarrow\; p^2 + (p+1)^2 = a^2.$$

По определению 1.1 тройка $(p; p+1; a)$ является пифагоровой. Используя теорему 1.1, построим систему уравнений с двумя неизвестными m, n с параметром p:

$$\begin{cases} m^2 - n^2 = p \\ 2mn = p + 1. \end{cases}$$

Выясним, при каких значениях параметра $p \in \mathbb{P}$ эта система имеет решение в натуральных числах m, n.

$$\begin{cases} m^2 - n^2 = p \\ 2mn = p+1 \end{cases} \Leftrightarrow \begin{cases} (m+n)\cdot(m-n) = p \\ 2mn = p+1 \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} \left[\begin{array}{l} \begin{cases} m+n = p \\ m-n = 1 \end{cases} \\ \begin{cases} m+n = 1 \\ m-n = p \end{cases} \end{array} \right. \\ 2mn = p+1 \end{cases} \overset{m+n>1}{\Leftrightarrow} \begin{cases} m+n = p \\ m-n = 1 \\ 2mn = p+1 \end{cases} \Leftrightarrow \begin{cases} 2m = p+1 \\ m-n = 1 \\ (2m)\cdot n = p+1 \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} p = 2m-1 \\ m = n+1 \\ (p+1)\cdot n = p+1 \end{cases} \Leftrightarrow \begin{cases} p = 3 \\ m = 2 \\ n = 1\ . \end{cases}$$

В свою очередь, по теореме 1.1, $m^2 + n^2 = a$. Значит, $a = 5$. Делаем вывод:

$$2p(p+1)+1 = a^2 \quad \Leftrightarrow \quad p = 3 \quad \wedge \quad a = 5.$$

В таком случае будет верно утверждение

$$(\forall p \in \mathbb{P}\setminus\{3\})(\forall a \in \mathbb{N})(2p(p+1)+1 \neq a^2).$$

В конечном итоге,

$$(\forall p \in \mathbb{P})(\forall a \in \mathbb{N})(2p+1 \neq a^2) \ \wedge$$

$$\wedge \ (\forall p \in \mathbb{P})(\forall a \in \mathbb{N})(2p(p+1) \neq a^2) \ \wedge$$

$$\wedge \ (\forall p \in \mathbb{P}\setminus\{3\})(\forall a \in \mathbb{N})(2p(p+1)+1 \neq a^2) \quad \Rightarrow$$

$$\Rightarrow \quad (\forall p \in \mathbb{P}\setminus\{3\})(\forall a \in \mathbb{N})(2p+1 \neq a^2) \ \wedge$$

$$\wedge \ (\forall p \in \mathbb{P}\setminus\{3\})(\forall a \in \mathbb{N})(2p(p+1) \neq a^2) \ \wedge$$

$$\wedge \ (\forall p \in \mathbb{P}\setminus\{3\})(\forall a \in \mathbb{N})(2p(p+1)+1 \neq a^2) \quad \Leftrightarrow$$

$$\Leftrightarrow \quad (\forall p \in \mathbb{P}\setminus\{3\})(\forall a \in \mathbb{N})(2p+1 \neq a^2 \quad \wedge \quad 2p(p+1) \neq a^2 \quad \wedge \quad 2p(p+1)+1 \neq a^2).$$

Утверждение 4.2 доказано.

Геометрически утверждение 4.2 означает, что у примитивного пифагорового треугольника $(x; y; y+1)$, в которого вписана окружность с простым радиусом $p \neq 3$, все стороны не представимы в виде полного квадрата.

СЛЕДСТВИЕ 4.3. Для любого простого числа Софи Жермен $p^* \neq 3$ все составляющие элементов множества F^* не являются полными квадратами.

5. Геометрическое построение примитивных пифагоровых треугольников $(x; y; y+1)$

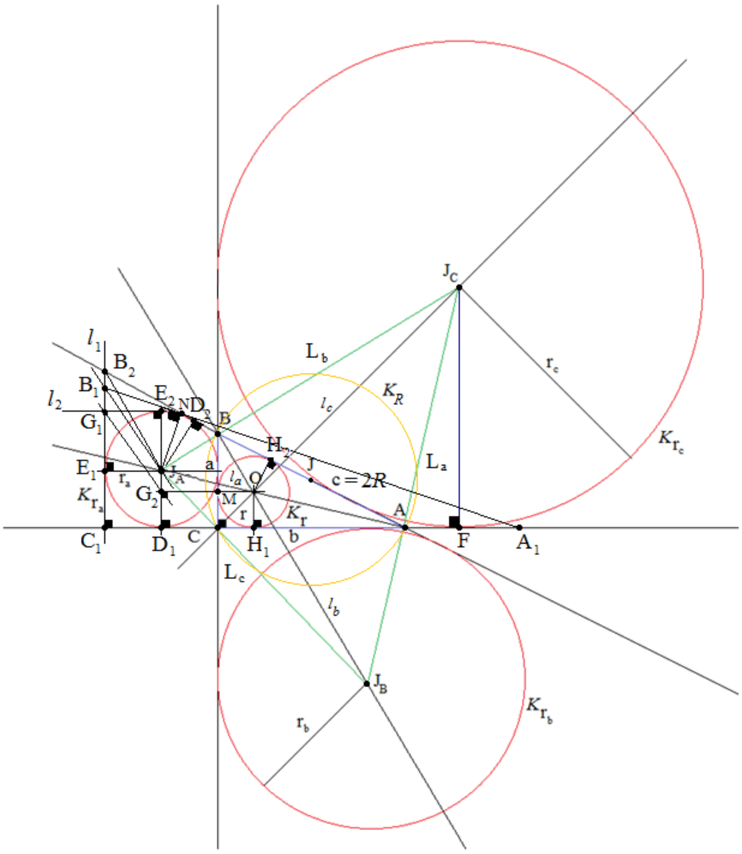


рис. 4

Будем считать, что рис. 3 построен для примитивного пифагорового треугольника ΔACB.

В дальнейшем для вычисления сторон некоторых прямоугольных треугольников будем использовать теорему Пифагора. На стадии подготовки построения новых примитивных пифагоровых треугольников $(x; y; y+1)$ на основе заданного примитивного пифагорового треугольника ΔACB нам пригодятся следующие известные теоремы (см. [6], [7]).

ТЕОРЕМА 5.1. Касательная к окружности перпендикулярна радиусу, проведённому в точку касания (см. рис. 5).

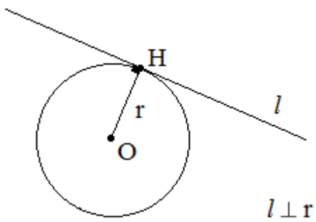
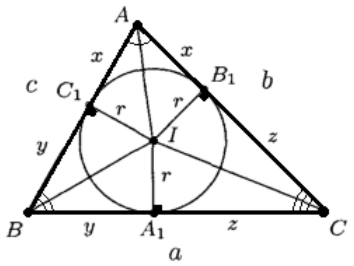


рис. 5

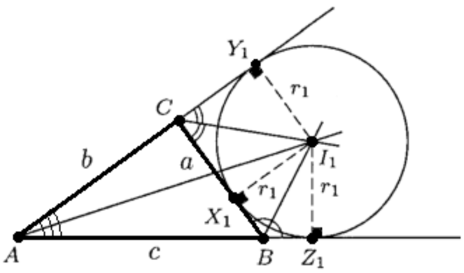
ТЕОРЕМА 5.2. В любом треугольнике расстояние от вершины треугольника до точки касания вписанной окружности со стороной треугольника, выходящей из данной вершины, есть разность полупериметра треугольника и стороны, противолежащей данной вершине (см. рис. 6).



$$x = s - a,\quad y = s - b,\quad z = s - c,\ \text{где}\ s = \frac{a+b+c}{2}.$$

рис. 6

ТЕОРЕМА 5.3. В любом треугольнике расстояние от вершины треугольника до точки касания вневписанной окружности с продолжением стороны треугольника, выходящей из данной вершины, есть полупериметр треугольника (см. рис. 7).



$$AY_1 = AZ_1 = s,\quad \text{где}\ s = \frac{a+b+c}{2}.$$

рис. 7

ТЕОРЕМА 5.4 (теорема о парах параллельных прямых). Пусть пара параллельных прямых AB и CD пересекает соответственно другую пару параллельных прямых AC и BD. Тогда отрезок AB равен отрезку CD, а отрезок AC равен отрезку BD (см. рис. 8).

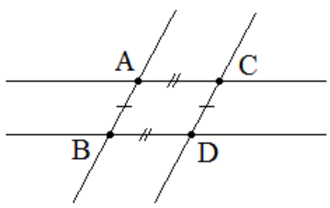


рис. 8

Подготовка (см. рис. 4). Этап 1. Проведём касательную l_1 к окружности K_{r_a}, параллельную катету BC треугольника ΔACB. Тогда касательная l_1 пересекается с продолжением сторон AB и AC треугольника ΔACB соответственно в точках B_2 и C_1. В результате образуется прямоугольный треугольник ΔAC_1B_2 с катетами AC_1, B_2C_1 и гипотенузой AB_2.

Пусть M – точка касания отрезка BC (касательной BC) с окружностью K_r;

E_1 – точка касания отрезка B_2C_1 касательной l_1 с окружностью K_{r_a}.

Соединим центр J_A окружности K_{r_a} с точкой E_1, а центр O окружности K_r с точкой M. Тогда $J_AE_1 = r_a$, $OM = r$. По теореме 5.1, $B_2C_1 \perp J_AE_1$, $BC \perp OM$.

Этап 2. Пусть H_1 – точка касания отрезка AC с окружностью K_r;

H_2 – точка касания отрезка AB с окружностью K_r.

Соединим центр O окружности K_r с точками H_1, H_2. Тогда $OH_1 = OH_2 = r$.

По теореме 5.1, $AC \perp OH_1$, $AB \perp OH_2$. С учётом теоремы 5.2,

$$CH_1 = s - c = r,$$

$$AH_1 = AH_2 = s - a \overset{(19)}{=} r_b.$$

Исходя из равенств $CH_1 = r$, $AH_1 = AH_2$ и $c = b + 1$, получим $BH_2 = r + 1 \overset{(16)}{=} r_a$.

Этап 3. Пусть D_1 – точка касания отрезка AC_1 с окружностью K_{r_a};

D_2 – точка касания отрезка AB_2 с окружностью K_{r_a}.

Соединим центр J_A окружности K_{r_a} с точками D_1, D_2. Тогда $J_AD_1 = J_AD_2 = r_a$.

По теореме 5.1, $AC_1 \perp J_AD_1$, $AB_2 \perp J_AD_2$. Из теоремы 5.3 следует

$$AD_1 = AD_2 = s = r_c. \tag{21}$$

$$CD_1 = AD_1 - AC \overset{(21)}{=} s - b \overset{(19)}{=} r_a \;\Rightarrow\; CD_1 = r_a.$$

$$AD_2 = AD_1 \;\Leftrightarrow\; AH_2 + D_2H_2 = AH_1 + D_1H_1 \;\Leftrightarrow\; D_2H_2 = D_1H_1.$$

$$D_1H_1 = AD_1 - AH_1 \overset{(21)}{=} s - (s - a) = a \;\Rightarrow\; D_1H_1 = a.$$

Так как окружности K_r, K_{r_a} лежат по одну сторону от касательной D_1H_1, то длина отрезка общей касательной AC_1 к двум окружностям K_r, K_{r_a}, заключённого между точками касания D_1, H_1 находится по формуле $D_1H_1 = \sqrt{l_a^2 - (r_a - r)^2}$.

Расстояние l_a не является натуральным числом. Чтобы это явно показать, найдём расстояние l_a через катет a треугольника ΔACB.

$$D_1H_1 = \sqrt{l_a^2 - (r_a - r)^2} \overset{(16)}{\Leftrightarrow} a = \sqrt{l_a^2 - (r + 1 - r)^2} \;\Leftrightarrow$$

$$\Leftrightarrow\; a = \sqrt{l_a^2 - 1} \;\Leftrightarrow\; a^2 = l_a^2 - 1 \;\Rightarrow\; l_a = \sqrt{a^2 + 1} \notin \mathbb{N}.$$

Применяя первую формулу из утверждения 3.5 и базовое соотношение (20), указанное в его доказательстве, упростим формулу вычисления расстояния AO от вершины A треугольника ΔACB до центра O вписанной в этот же треугольник окружности K_r.

$$AO \cdot l_a = 4Rr \;\Leftrightarrow\; AO = \tfrac{4Rr}{l_a}.$$

$$AO = \frac{2\cdot(2R)\cdot r}{l_a} = \frac{(2c)\cdot r}{l_a} = \frac{l_a^2\cdot r}{l_a} = l_a \cdot r \;\Rightarrow\; AO = l_a \cdot r.$$

Расстояние AJ_A от вершины A треугольника ΔACB до центра J_A вневписанной окружности K_{r_a} этого же треугольника можно вычислить так:

$$AJ_A = AO + OJ_A = l_a \cdot r + l_a = l_a \cdot (r+1) \overset{(16)}{=} l_a \cdot r_a \;\Rightarrow$$

$$\Rightarrow\; AJ_A = l_a \cdot r_a.$$

Вывод 5.1. Отрезки OJ_A, AO, AJ_A пропорциональны катету a треугольника ΔACB, радиусу r_b окружности K_{r_b} и радиусу r_c окружности K_{r_c}, то есть верны геометрические пропорции:

$$\frac{OJ_A}{a} = \frac{AO}{r_b} = \frac{AJ_A}{r_c}.$$

Так как $l_a \notin \mathbb{N}$, расстояния AO и AJ_A не являются натуральными числами.

Этап 4. Пара параллельных прямых C_1D_1 и J_AE_1 пересекает соответственно другую пару параллельных прямых E_1C_1 и J_AD_1. Тогда по теореме 5.4 отрезок C_1D_1 равен отрезку J_AE_1, а отрезок E_1C_1 равен отрезку J_AD_1. Более того, $C_1D_1 = E_1C_1 = r_a$.

Окружность K_{r_a} является вписанной в треугольник ΔAC_1B_2 окружностью. Поэтому из теоремы 5.2 следует равенство $B_2D_2 = B_2E_1$.

Выразим длины сторон треугольника ΔAC_1B_2, используя полученные равенства.

$$AC_1 = AD_1 + C_1D_1 \overset{(21)}{=} r_c + r_a.$$

$$B_2C_1 = B_2E_1 + E_1C_1 = B_2E_1 + r_a.$$

$$AB_2 = AD_2 + B_2D_2 \overset{(21)}{=} r_c + B_2E_1.$$

Теперь требуется вычислить длину отрезка B_2E_1, лежащего на катете B_2C_1 треугольника ΔAC_1B_2. Для этого решаем уравнение относительно неизвестного B_2E_1, полученное из теоремы Пифагора для треугольника ΔAC_1B_2. Тем самым найдём длину катета B_2C_1 и длину гипотенузы AB_2 треугольника ΔAC_1B_2.

$$AC_1^2 + B_2C_1^2 = AB_2^2 \quad\Leftrightarrow$$

$$\Leftrightarrow\quad (r_c + r_a)^2 + (B_2E_1 + r_a)^2 = (r_c + B_2E_1)^2 \quad\Leftrightarrow$$

$$\Leftrightarrow\quad r_c^2 + 2\cdot r_c \cdot r_a + r_a^2 + B_2E_1^2 + 2\cdot B_2E_1 \cdot r_a + r_a^2 =$$

$$= r_c^2 + 2\cdot r_c \cdot B_2E_1 + B_2E_1^2 \quad\Leftrightarrow$$

$$\Leftrightarrow\quad 2\cdot r_c \cdot r_a + 2\cdot r_a^2 + 2\cdot B_2E_1 \cdot r_a = 2\cdot r_c \cdot B_2E_1 \quad\Leftrightarrow$$

$$\Leftrightarrow \quad r_c + r_a + B_2E_1 = \left(\frac{r_c}{r_a}\right) \cdot B_2E_1 \overset{(16)}{\Leftrightarrow}$$

$$\Leftrightarrow \quad a \cdot r_a + r_a + B_2E_1 = \left(\frac{a \cdot r_a}{r_a}\right) \cdot B_2E_1 \quad \Leftrightarrow$$

$$\Leftrightarrow \quad (a-1) \cdot B_2E_1 = r_a \cdot (a+1) \quad \Leftrightarrow \quad B_2E_1 = r_a \cdot \left(\frac{a+1}{a-1}\right).$$

$$B_2E_1 = r_a \cdot \left(\frac{a+1}{a-1}\right) = r_a \cdot \left(\frac{(2r+1)+1}{(2r+1)-1}\right) = r_a \cdot \left(\frac{2 \cdot (r+1)}{2r}\right) =$$

$$= r_a \cdot \left(\frac{r+1}{r}\right) \overset{(16)}{=} \frac{r_a^2}{r} \quad \Rightarrow \quad B_2E_1 = \frac{r_a^2}{r}.$$

В итоге, ΔAC_1B_2:

$$AC_1 = r_a + r_c \quad \wedge \quad B_2C_1 = r_a + \frac{r_a^2}{r} \quad \wedge \quad AB_2 = r_c + \frac{r_a^2}{r}. \tag{22}$$

Этап 5. Проведём касательную l_2 к окружности K_{r_a}, параллельную катету AC_1 треугольника ΔAC_1B_2. При этом прямая l_2 пересекается с катетом B_2C_1 треугольника ΔAC_1B_2 в точке G_1.

Пусть E_2 – точка касания прямой l_2 с окружностью K_{r_a}. Соединим центр J_A окружности K_{r_a} с точкой E_2. В этом случае, $J_AE_2 = r_a$. По теореме 5.1, $G_1E_2 \perp J_AE_2$.

Пара параллельных прямых G_1E_2 и C_1D_1 пересекает соответственно другую пару параллельных прямых C_1G_1 и E_2D_1. Тогда по теореме 5.4 отрезок G_1E_2 равен отрезку C_1D_1, а отрезок C_1G_1 равен отрезку E_2D_1.

$$G_1E_2 = C_1D_1 \quad \wedge \quad C_1D_1 = r_a \quad \Rightarrow \quad G_1E_2 = r_a.$$

$$C_1G_1 = E_2D_1 = J_AE_2 + J_AD_1 = r_a + r_a = 2r_a \quad \Rightarrow \quad C_1G_1 = 2r_a. \tag{23}$$

УТВЕРЖДЕНИЕ 5.5.

$$2r_a + 1 < B_2C_1.$$

ДОКАЗАТЕЛЬСТВО.

$$r < r_a \quad \Leftrightarrow \quad \frac{1}{r_a} < \frac{1}{r} \quad \Leftrightarrow \quad 2 + \frac{1}{r_a} < 2 + \frac{1}{r} \quad \Leftrightarrow$$

$$\Leftrightarrow \quad 2 + \frac{1}{r_a} < 1 + \frac{r+1}{r} \overset{(16)}{\Leftrightarrow} 2 + \frac{1}{r_a} < 1 + \frac{r_a}{r} \quad \Leftrightarrow$$

$$\Leftrightarrow \quad 2r_a + 1 < r_a + \frac{r_a^2}{r} \overset{(22)}{\Leftrightarrow} 2r_a + 1 < B_2C_1.$$

Утверждение 5.5 доказано.

Из утверждения 5.5 следует, что на отрезке B_2G_1 катета B_2C_1 треугольника ΔAC_1B_2 существует точка B_1, такая, что $B_1C_1 = 2r_a + 1$.

Этап 6. Отметим точку B_1 следующим образом. Опустим перпендикуляр OG_2 с центра O окружности K_r на радиус J_AD_1 окружности K_{r_a}. В результате образуется прямоугольник $G_2OH_1D_1$, где $G_2D_1 = OH_1 = r$. Перпендикуляр OG_2 пересекает катет BC треугольника ΔACB в точке M.

$$J_AG_2 = J_AD_1 - G_2D_1 = r_a - r = 1 \;\;\Rightarrow\;\; J_AG_2 = 1.$$

Проведём прямую G_2G_1, проходящую через точки G_2 и G_1. Проведём прямую J_AB_1, проходящую через точку J_A и параллельную прямой G_2G_1. Тогда прямая J_AB_1 пересекает катет B_2C_1 треугольника ΔAC_1B_2 в точке B_1.

Пара параллельных прямых G_2G_1 и J_AB_1 пересекает соответственно другую пару параллельных прямых J_AG_2 и B_1G_1. Тогда по теореме 5.4 отрезок G_2G_1 равен отрезку J_AB_1, а отрезок J_AG_2 равен отрезку B_1G_1.

$$B_1G_1 = J_AG_2 \;\;\wedge\;\; J_AG_2 = 1 \;\;\Rightarrow\;\; B_1G_1 = 1.$$

$$B_1C_1 = C_1G_1 + B_1G_1 \overset{(23)}{=} 2r_a + 1.$$

Этап 7. Опустим из центра J_C окружности K_{r_c} на продолжение стороны AC треугольника ΔACB перпендикуляр J_CF. Из теоремы 5.3 следует, что $CF = s$.

$$AF = CF - AC = s - b \overset{(19)}{=} r_a.$$

Этап 8. Отметим на продолжении стороны AC треугольника ΔACB точку A_1, симметричную точке A относительно точки F – центра симметрии. Тогда

$$A_1F = AF = r_a.$$

Соединяя точки A_1 и B_1, в итоге построим примитивный пифагоров треугольник $\Delta A_1C_1B_1$ с катетами A_1C_1, B_1C_1 и гипотенузой A_1B_1:

$$A_1C_1 = AC_1 + AF + A_1F \overset{(22)}{=} (r_a + r_c) + r_a + r_a =$$

$$= 3r_a + r_c \overset{(16)}{=} 3r_a + ar_a = (a+3)\cdot r_a = (2r+4)\cdot r_a =$$

$$= 2\cdot(r+2)\cdot r_a \overset{(16)}{=} 2\cdot(r_a+1)\cdot r_a \;\Rightarrow\; A_1C_1 = 2r_a\cdot(r_a+1) \in \mathbb{N}.$$

$$B_1C_1 = 2r_a + 1 \in \mathbb{N}.$$

По теореме Пифагора, $A_1B_1^2 = A_1C_1^2 + B_1C_1^2$.

$$A_1B_1^2 = (2\cdot r_a\cdot(r_a+1))^2 + (2r_a+1)^2 =$$

$$= (2\cdot r_a\cdot(r_a+1))^2 + 4r_a^2 + 4r_a + 1 =$$

$$= (2\cdot r_a\cdot(r_a+1))^2 + 2\cdot(2\cdot r_a\cdot(r_a+1)) + 1 =$$

$$= (2\cdot r_a\cdot(r_a+1)+1)^2 \;\Rightarrow\; A_1B_1^2 = (2\cdot r_a\cdot(r_a+1)+1)^2 \;\Rightarrow$$

$$\Rightarrow\; A_1B_1 = 2\cdot r_a\cdot(r_a+1)+1 \in \mathbb{N}.$$

Окружность K_{r_a} вписана в прямоугольный треугольник $\Delta A_1C_1B_1$, так как

$$r_a = \frac{B_1C_1 + A_1C_1 - A_1B_1}{2}.$$

Значит, каждая сторона треугольника $\Delta A_1C_1B_1$ касается окружности K_{r_a} в единственной точке. Гипотенуза A_1B_1 треугольника $\Delta A_1C_1B_1$ касается окружности K_{r_a} в точке N.

Подготовка завершена.

Геометрическое построение примитивных пифагоровых треугольников $(x; y; y+1)$**.**

Пусть задан примитивный пифагоров треугольник ΔACB:

$$BC = 2r + 1,\ AC = 2r \cdot (r+1),\ \ AB = 2r \cdot (r+1) + 1,\ r \in \mathbb{N}.$$

Шаг 1. Создаём рисунок рис. 3 для заданного треугольника ΔACB.

Шаг 2. Проведём касательную l_1 к окружности K_{r_a}, параллельную катету BC треугольника ΔACB. Тогда прямая l_1 пересекается с продолжением сторон AB и AC треугольника ΔACB соответственно в точках B_2 и C_1.

Шаг 3. Опустим с центра J_A окружности K_{r_a} перпендикуляр J_AD_1 на продолжение стороны AC треугольника ΔACB.

Шаг 4. Опустим с центра O окружности K_r перпендикуляр OG_2 на радиус J_AD_1 окружности K_{r_a}.

Шаг 5. Проведём касательную l_2 к окружности K_{r_a}, параллельную катету AC треугольника ΔACB. При этом прямая l_2 пересекается с прямой l_1 в точке G_1.

Шаг 6. Проведём луч G_2G_1 и луч J_AB_1, параллельный лучу G_2G_1. При этом луч J_AB_1 пересекает прямую l_1 в точке B_1.

Шаг 7. Опустим с центра J_C окружности K_{r_c} перпендикуляр J_CF на продолжение стороны AC треугольника ΔACB.

Шаг 8. Отметим на продолжении стороны AC треугольника ΔACB точку A_1, симметричную точке A относительно точки F.

Шаг 9. Соединяем точки A_1 и B_1. В результате получаем примитивный пифагоров треугольник $\Delta A_1C_1B_1$:

$$B_1C_1 = 2r_a + 1,\ A_1C_1 = 2r_a \cdot (r_a + 1),\ \ A_1B_1 = 2r_a \cdot (r_a + 1) + 1.$$

6. Заключение

Результаты, полученные в данной статье, являются отправной точкой в исследовании примитивных пифагоровых треугольников, у которых меньший катет равен безопасному простому числу. Выявление геометрической закономерности в этих треугольниках считается ключевым решением гипотезы Софи Жермен. Решение этой задачи геометрическим способом позволит посмотреть на объекты планиметрии по-другому и ответить на многие вопросы теории чисел, связанные с простыми числами разных видов.

СПИСОК ЛИТЕРАТУРЫ

[1] В. Серпинский. Пифагоровы треугольники. – М.: Учпедгиз, 1959. – 111 с.

[2] P. Ribenboim, The Little Book of Bigger Primes, Springer-Verlag, New York, 2004.

[3] Белоусов А.И., Ткачев С.Б. Дискретная математика: Учеб. для вузов / Под ред. В.С. Зарубина, А.П. Крищенко. – 3-е изд., стереотип. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2004. – 744 с. (Сер. Математика в техническом университете; Вып. XIX).

[4] Donald E. Knuth. The Art of Computer Programming, Volume 2: Seminumeral Algorithms. Addison-Wesley, third edition, 1998.

[5] Ramin Takloo-Bighash. A Pythagorean Introduction to Number Theory. Right Triangles, Sums of Squares, and Arithmetic. Undergraduate Texts in Mathematics. Springer Verlag, 2018.

[6] L. Debnath. The Legacy of Leonhard Euler: A Tricentennial Tribute (London, 2010).

[7] Понарин Я. П. Элементарная геометрия: В 2 т. – Т. 1: Планиметрия, преобразования плоскости. – М.: МЦНМО, 2004. – 312 с.

[8] Корн Г., Корн Т. Справочник по математике для научных работников и инженеров. Определения, теоремы, формулы. Перев. с англ. – М.: Наука, 1973. – 832 с.