УДК 510.52, 511.213, 511.216, 519.688

П. Г. Емельянов

ВОССТАНОВЛЕНИЕ ПУТИ В ДЕРЕВЕ БАРНИНГА – ХОЛЛА

В 1963 г. Ф. Дж. М. Барнинг и в 1970 г. А. Холл описали систематическую процедуру порождения всех примитивных пифагоровых троек с помощью умножения минимальной пифагоровой тройки $[3, 4, 5]$, рассматриваемой как вектор, на последовательность матриц, выбираемых из фиксированного трехэлементного множества унимодулярных матриц. Тем самым на множестве примитивных пифагоровых троек задается структура бесконечного тернарного корневого помеченного дерева. В данной работе представлен алгоритм, который по заданной примитивной пифагоровой тройке (ППТ) строит путь в этом дереве, ведущий от корня к этой тройке. Так как тройка может лежать очень глубоко, эффективность алгоритма имеет первостепенное значение. Представленный алгоритм имеет полиномиальную временную сложность относительно длины входа, которая соответствует логарифму некоторой величины, характеризующей размер ППТ.

Ключевые слова: пифагоровы тройки, дерево Барнинга – Холла, генераторы троек, восстановление пути, эффективность алгоритма.

1. Пифагоровы тройки

Пифагоровой тройкой (ПТ) называется тройка целых чисел $[x, y, z]$, удовлетворяющая следующему тождеству:

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

Тройка называется примитивной (ППТ), если ее элементы взаимно просты: $(x, y, z) = 1$. Далее будут рассматриваться только примитивные тройки и полагаться, что они упорядочены, их элементы положительны, четный элемент находится на втором месте. Минимальной ППТ является $[3, 4, 5]$. В зависимости от контекста тройки будут рассматриваться как вектора; для краткости знак транспонирования указываться не будет.

Традиционным изображением множества ППТ является их размещение на плоскости (см. рис. 1; для симметризации картинки приведены также тройки, полученные из $[4, 3, 5]$), с использованием в качестве координат значений первой и второй компоненты. В этом случае третья компонета описывает расстояние от центра координат.

Теорема 1. *Все ППТ описываются следующей параметризацией:*

$$[x, y, z] = [t^2 - s^2, 2ts, t^2 + s^2],$$

где $0 < s < t, (t, s) = 1, t \not\equiv s \pmod 2$.

В 1963 г. в отчете Амстердамского математического центра Ф. Дж. М. Барнинг [1] описал систематическую процедуру порождения ППТ. Отчет был написан на голландском языке и не получил широкой известности. Этот результат был переоткрыт в 1970 г. А. Холлом [2].

ISSN 1818-7897. Вестник НГУ. Серия: Математика, механика, информатика. 2012. Т. 12, вып. 3. С. 95–102

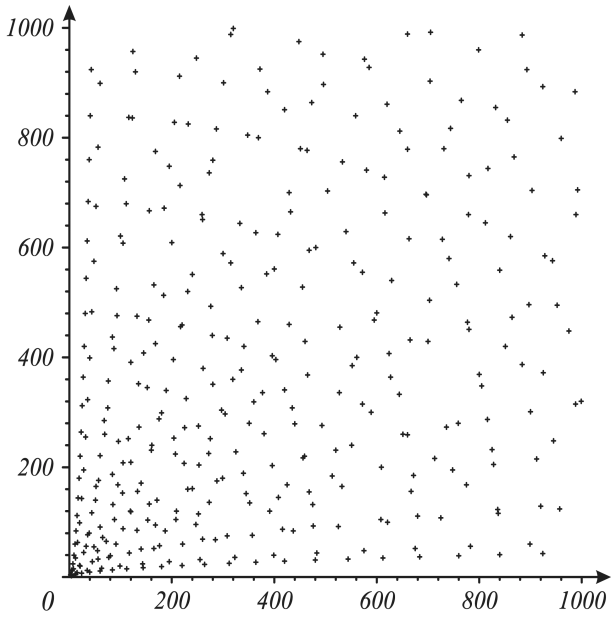

Рис. 1. Примитивные пифагоровы тройки

Теорема 2. *Всякая ППТ* $[x, y, z]$ *может быть получена из минимальной ППТ* $[3, 4, 5]$ *последовательным умножением на унимодулярные матрицы:*

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \mathbf{M}_k \dots \mathbf{M}_2 \mathbf{M}_1 \begin{bmatrix} 3 \\ 4 \\ 5 \end{bmatrix},$$

где $\mathbf{M}_i \in \mathcal{T} = \{\mathbf{A}, \mathbf{B}, \mathbf{C}\}$,

$$\mathbf{A} = \begin{bmatrix} -1 & 2 & 2 \\ -2 & 1 & 2 \\ -2 & 2 & 3 \end{bmatrix} \bigwedge \quad \mathbf{B} = \begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{bmatrix} \quad \mathbf{C} = \begin{bmatrix} 1 & -2 & 2 \\ 2 & -1 & 2 \\ 2 & -2 & 3 \end{bmatrix}.$$

Замечание 1. $\mathbf{A}, \mathbf{C} \in \mathbb{SL}_3(\mathbb{Z}) \subset \mathbb{GL}_3(\mathbb{Z}), \mathbf{B} \in \mathbb{GL}_3(\mathbb{Z})$.

Решение задачи об отыскании пути опирается на утверждение, доказательство которого для автора было инспирировано изображением на рис. 2.

Утверждение 1. *Если* $[x, y, z]$ *— ППТ, и* $\mathbf{M} \in \mathcal{T}$*, то для ее образа*

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = \mathbf{M} \begin{bmatrix} x \\ y \\ z \end{bmatrix}$$

верно

$$\begin{array}{lllll} 0 & < & \frac{X}{Y} & < & \frac{3}{4} \quad \textit{для} \quad \mathbf{M} = \mathbf{C}, \\ \frac{3}{4} & < & \frac{X}{Y} & < & \frac{4}{3} \quad \textit{для} \quad \mathbf{M} = \mathbf{B}, \\ \frac{4}{3} & < & \frac{X}{Y} & & \quad \textit{для} \quad \mathbf{M} = \mathbf{A}. \end{array}$$

ДОКАЗАТЕЛЬСТВО. Пусть $\mathbf{M} = \mathbf{B}$ (остальные преобразования из $\mathcal{T}$ рассматриваются аналогично) и

$$[x, y, z] = [t^2 - s^2, 2ts, t^2 + s^2],$$

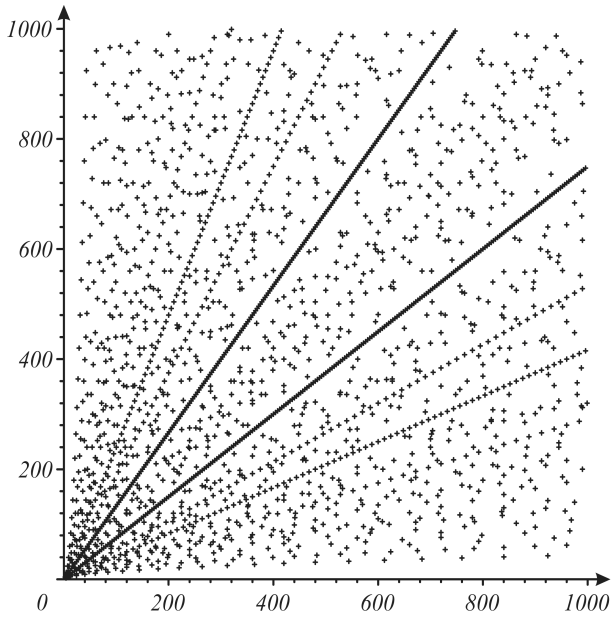

Рис. 2. Непримитивные пифагоровы тройки

где $0 < s < t, (t,s) = 1, t \not\equiv s \pmod 2$. Тогда $[X,Y,Z] = [3t^2 + 4ts + s^2,\ 4t^2 + 2ts,\ 5t^2 + 4ts + s^2]$. Минимизация и максимизация

$$\frac{3t^2 + 4ts + s^2}{4t^2 + 2ts}$$

при условии $0 < s < t$ дает требуемое утверждение. □

Замечание 2. Аналогичные секторы в первом квадранте плоскости, определяемой первыми двумя компонентами пифагоровых троек, задают и произведения матриц из $\mathcal{T}$. Для произведений длины k таких секторов будет 3^k. Например, всякая ППТ будет переводиться преобразованием **CAB** в сектор, определяемый неравенством $\frac{33}{56} < \frac{X}{Y} < \frac{28}{45}$. Разбиение первого квадранта на секторы-«аттракторы» для произведений матриц из $\mathcal{T}$ вычисляется с помощью простого алгоритма: нижняя граница для сектора определяется ППТ, которая получается умножением соответствующей матрицы на вектор $[1,0,1]$ или $[0,1,1]$ в зависимости от того, нечетное или четное число раз входит матрица **B** в произведение.

Нас интересует задача построения по заданной ППТ пути, который ведет из корня дерева Барнинга–Холла в вершину, соответствующую заданной тройке. Обнаружив свойства преобразований **A**, **B**, **C** из утверждения 1, авторы, например, [3], утверждают, что далее решение задачи тривиально. Действительно, зная, какому сектору принадлежит отношение первых двух компонент ППТ, можно определить, какое из отображений было применено последним. Так как все отображения обратимы (матрицы унимодулярны), можно получить предшествующую (на пути из корня дерева) ППТ. Повторяя этот процесс до достижения минимальной ППТ $[3,4,5]$, в конце концов мы построим искомый путь. Однако, хотя процедура сама по себе является очень простой, количество шагов может быть велико. Как будет показано ниже, оно варьируется в диапазоне от $\Omega(\log N)$ до $\Omega(\sqrt{N})$, где N — некоторая величина, естественным образом характери-

зующая размер ППТ. Например, в качестве такой величины можно выбрать значение третьей (наибольшей из всех) компоненты ППТ: $N = t^2 + s^2$.

2. От троек к парам

Хотя для решения поставленной задачи рассуждения, приведенные в п. 3, можно провести непосредственно для самих ППТ (забегая вперед: в этом случае вместо прямых будут фигурировать параболы), мы перейдем к новому дереву, изоморфному дереву Барнинга–Холла. Это упрощает нотацию и рассуждения и делает алгоритм более эффективным с вычислительной точки зрения. Новое дерево — это дерево параметров-генераторов ППТ: $[t, s] \mapsto [t^2 - s^2, 2ts, t^2 + s^2], 0 < s < t, (t, s) = 1, t \not\equiv s \pmod 2$.

В литературе имеются ссылки на работу A. P. Канга [4], где приведен метод порождения пар-генераторов, рассматриваемый ниже. К сожалению, автору эта работа оказалась недоступна, поэтому он приводит доказательство.

Теорема 3. *Всякая пара* $\pi = [t, s]$, *где* $0 < s < t$, $(t, s) = 1$, $t \not\equiv s \pmod 2$, *может быть получена из минимальной пары* $\pi_0 = [2, 1]$ *последовательным умножением на матрицы:*

$$\pi = M_k \dots M_2 M_1 \pi_0,$$

где $M_i \in \mathcal{P} = \{A, B, C\}$,

$$A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}, \quad C = \begin{bmatrix} 2 & -1 \\ 1 & 0 \end{bmatrix}.$$

ДОКАЗАТЕЛЬСТВО. Доказательство является простым следствием теоремы о параметризации ППТ и теоремы Барнинга–Холла. Установим соответствие между элементами $\mathcal{T}$ и $\mathcal{P}$. Рассмотрим переход от одной ППТ к другой под действием некоторого преобразования из $\mathcal{T}$, например $\mathbf{B}$ (другие — аналогично):

$$\begin{bmatrix} T^2 - S^2 \\ 2TS \\ T^2 + S^2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{bmatrix} \begin{bmatrix} t^2 - s^2 \\ 2ts \\ t^2 + s^2 \end{bmatrix}.$$

Выбрав любую пару тождеств между компонентами (третья является зависимой) и решив эту систему уравнений относительно T и S, имеем:

$$T = 2t + s, \quad S = t,$$

что соответствует умножению на матрицу B. □

Замечание 3. $A, C \in \mathbb{SL}_2(\mathbb{Z}) \subset \mathbb{GL}_2(\mathbb{Z}), B \in \mathbb{GL}_2(\mathbb{Z})$. Отметим, что $A = \mathbf{TT}$ и $C = \mathbf{TTS}$, где $\mathbf{T}$ и $\mathbf{S}$ — стандартные порождающие элементы (перенос вдоль оси абсцисс и ортогональный поворот соответственно) специальной линейной группы $\mathbb{SL}_2(\mathbb{Z})$.

Таким образом, получен систематический способ порождения взаимно-простых пар чисел противоположной четности. Он задает бесконечное тернарное корневое помеченное дерево, изоморфное дереву Барнинга–Холла.

Для пар также справедливо соответствующее «секторное» утверждение (доказательство его аналогично доказательству для ППТ).

Утверждение 2. *Если $\pi = [t, s]$ — пара, и $M \in \mathcal{P}$, то для ее образа*

$$\begin{bmatrix} T \\ S \end{bmatrix} = M \begin{bmatrix} t \\ s \end{bmatrix}$$

верно

$$\begin{array}{rcccl} 0 & < & \frac{S}{T} & < & \frac{1}{3} \quad \textit{для} \quad M = A, \\ \frac{1}{3} & < & \frac{S}{T} & < & \frac{1}{2} \quad \textit{для} \quad M = B, \\ \frac{1}{2} & < & \frac{S}{T} & < & 1 \quad \textit{для} \quad M = C. \end{array}$$

В дальнейшем M-сектор — это сектор, соответствующий преобразованию $M \in \mathcal{P}$. Верхняя/нижняя граница сектора — это соответствующий луч. Никакая пара, за исключением $\pi_0 = [2, 1]$, не лежит на границах секторов.

Интерес представляет поведение степеней преобразований из $\mathcal{P}$.

Утверждение 3.

$$A^k = \begin{bmatrix} 1 & 2k \\ 0 & 1 \end{bmatrix}, \qquad C^k = \begin{bmatrix} k+1 & -k \\ k & -k+1 \end{bmatrix},$$

$$B^k = \frac{1}{4} \begin{bmatrix} \Theta^k(2+\sqrt{2}) + \theta^k(2-\sqrt{2}) & \sqrt{2}(\Theta^k - \theta^k) \\ \sqrt{2}(\Theta^k - \theta^k) & \Theta^k(2-\sqrt{2}) + \theta^k(2+\sqrt{2}) \end{bmatrix},$$

где $\Theta = 1 + \sqrt{2}$ *и* $\theta = -\Theta^{-1} = 1 - \sqrt{2}$.

$$A^{-k} = \begin{bmatrix} 1 & -2k \\ 0 & 1 \end{bmatrix}, \qquad C^{-k} = \begin{bmatrix} -k+1 & k \\ -k & k+1 \end{bmatrix}.$$

Чтобы получить B^{-k}, нужно переставить элементы главной диагонали B^k местами и взять их с обратным знаком (это простое следствие унимодулярности матриц).

Отметим геометрическое расположение пар, порождаемых степенями преобразований A и C. Для любой пары π пары $A^k\pi$ и $C^k\pi$ располагаются на лучах, начинающихся в точке π и растущих параллельно оси абсцисс и биссектрисы первого координатного угла соответственно в направлении роста координат(ы).

Рассмотрим экстремальные относительно длины пути от корня случаи «залегания» ППТ. В качестве размера ППТ рассматривается третья компонента, что равно квадрату евклидовой нормы вектора, соответствующего паре-генератору π_M: $N_M = \|\pi_M\|^2$. Изменение нормы результирующего вектора при фиксированном начальном определяется максимальным собственным числом матрицы. Так как

$$\lambda_{\max}(A^k) = \lambda_{\max}(C^k) = 1, \quad \lambda_{\max}(B^k) = (1+\sqrt{2})^k,$$

то примерами медленно растущих пар будут $\pi_{A^k} = A^k\pi_0$ и $\pi_{C^k} = C^k\pi_0$, а быстро растущих — $\pi_{B^k} = B^k\pi_0$. Имеем:

$$N_{A^k} = 4k^2 + 8k + 5, \quad N_{C^k} = 2k^2 + 6k + 5, \quad N_{B^k} = \Omega((3+2\sqrt{2})^k).$$

Таким образом можно оценить диапазон длины пути в дереве: от $\Omega(\log N)$ до $\Omega(\sqrt{N})$. А значит, простейший алгоритм, использующий лишь утверждение 2, будет неэффективным. Если $L(N) = \log N$ — длина входа алгоритма, то оценка его временной сложности в худшем $O(2^{\text{const}\cdot L(N)})$, и эта оценка достижима, например, для π_{A^k} или π_{C^k}.

Для удобства оценивания скорости изменения пары $\pi = [t, s]$ в алгоритме восстановления пути рассмотрим величину $\|\pi\|_\infty = \max(|t|, |s|) = t$. Так как $\|\pi\|_\infty^2 < N < 2\|\pi\|_\infty^2$, то оценка сложности нашего алгоритма, доказанная «в терминах» t, будет справедливой и «в терминах» размера ППТ.

3. Исключение длинных последовательностей и сложность алгоритма

Идея улучшения эффективности алгоритма состоит в том, чтобы научиться быстро проходить участки пути, на которых «размер» пары изменяется медленно, т. е. для длинных последовательностей преобразований, состоящих только из A или только из C. Оказывается, это можно сделать за фиксированное число арифметических операций.

Пусть уже установлено, что текущая пара лежит в A-секторе. Максимальная последовательность преобразований A^k, ведущая в данную пару, начинается в паре, лежащей в секторе, отличном от A-сектора, а значит, прямая, проходящая через рассматриваемые пары, пересекает верхнюю границу этого сектора. Найдем пересечение:

$$A^{-k}\begin{bmatrix} t \\ s \end{bmatrix} = \begin{bmatrix} t - 2ks \\ s \end{bmatrix} = \begin{bmatrix} 3s \\ s \end{bmatrix}.$$

Выражая k, получаем:

$$k = \left\lceil \frac{t - 3s}{2s} \right\rceil.$$

Округление необходимо, так как нужно учесть, что пара-назначение лежит чуть дальше точки пересечения с границей сектора (в точке пересечения k рационально). Таким образом, отыскав k и применив преобразование A^{-k}, мы покинем A-сектор. Отметим, что все эти действия требуют фиксированного числа арифметических операций.

Для преобразования C ищется пересечение с нижней границей C-сектора:

$$C^{-k}\begin{bmatrix} t \\ s \end{bmatrix} = \begin{bmatrix} t - k(t - s) \\ s - k(t - s) \end{bmatrix} = \begin{bmatrix} 2\,(s - k(t - s)) \\ s - k(t - s) \end{bmatrix}.$$

Выражая k, получаем:

$$k = \left\lceil \frac{2s - t}{t - s} \right\rceil.$$

Для B ситуация сложнее из-за экспоненциальной зависимости компонент пар от количества последовательных применений преобразования. Действуя, как и в предыдущих случаях, имеем

$$\frac{s}{t} = \frac{\Theta^{k+1} + \theta^{k+1}}{\Theta^{k+2} + \theta^{k+2}} \quad \text{и} \quad \frac{s}{t} = \Theta \cdot \frac{\Theta^{k+2} + \theta^{k}}{\Theta^{k+4} - \theta^{k}}$$

для пересечения с нижней и верхней границами B-сектора соответственно, где, как и ранее, $\Theta = 1 + \sqrt{2}$ и $\theta = -\Theta^{-1} = 1 - \sqrt{2}$. При росте k обе величины в правых частях стремятся к $\sqrt{2} - 1$. Однако для доказательства полиномиальности алгоритма не требуется обращения соотношений для преобразования B.

Предшествующие рассуждения показывают, что, не уменьшая общности, можно считать, что рассматриваемый путь не содержит последовательностей преобразований A и

C длиной более единицы, т. е. двумя соседними одинаковыми преобразованиями могут быть только B. Завершающим шагом доказательства полиномиальности алгоритма построения пути в дереве будет демонстрация экспоненциального убывания (если рассматривать обратный ход к корню) или, что то же самое, роста (если рассматривать прямой ход от корня) параметра t. Таким образом, будет дана линейная оценка количества шагов алгоритма относительно длины входа — $O(L(t))$.

Пусть $[t_0, s_0] = [2, 1]$. Можно считать, что последовательность имеет четную длину (в противном случае в качестве базы индукции следует рассмотреть пары, получаемые из $[2, 1]$ применением одного преобразования из $\mathcal{P}$). $[t_{k+2}, s_{k+2}] = M[t_k, s_k]$, где $M \in \in \{AB,\ AC,\ BA,\ BB,\ BC,\ CA,\ CB\} = \mathcal{P}^2 \setminus \{AA, CC\}$. Докажем по индукции, что $t_k > 2^{\frac{k}{2}}$. Очевидно, что для $k = 0$ и любого преобразования M верно $t_0 > 1 = 2^0$. Пусть утверждение верно для k. Докажем его для $k + 2$. В этом случае порядок изменения первого параметра пары оценивается следующим образом:

M	$\frac{t_{k+2}}{t_k}$	$\inf\limits_{\frac{s_k}{t_k} \in (0,1)} \frac{t_{k+2}}{t_k}$
AB	$4 + \frac{s_k}{t_k}$	4
AC	$4 - \frac{s_k}{t_k}$	3
BA	$2 + 2\frac{s_k}{t_k}$	2
BB	$5 + 2\frac{s_k}{t_k}$	5
BC	$5 - 2\frac{s_k}{t_k}$	3
CA	$2 + 3\frac{s_k}{t_k}$	2
CB	$3 + 3\frac{s_k}{t_k}$	3

Это демонстрирует, что параметр t изменяется не менее чем в два раза. Таким образом, $t_{k+2} > 2\, t_k > 2\, 2^{\frac{k}{2}} = 2^{\frac{k}{2}+1} = 2^{\frac{k+2}{2}}$, и это завершает доказательство.

Список литературы

1. *Barning F. J. M.* Over Pythagorese en Bijna-Pythagorese Driehoeken en een Generatieproces met Behulp van Unimodulaire Matrices (On Pythagorean and Quasi-Pythagorean Triangles and a Generation Process with the Help of Unimodular Matrices): Afdeling Zuivere Wiskunde ZW 1963-011. Amsterdam: Mathematisch Centrum, 1963. (In Dutch).

2. *Hall A.* Genealogy of Pythagorean Triads // Mathematical Gazette. 1970. Vol. 54. No. 390. P. 377–379.

3. *Romik D.* The Dynamics of Pythagorean Triples // Trans. AMS. 2008. Vol. 360. P. 6045–6064.

4. *Kanga A. R.* The Family Tree of Pythagorean Triples // Bulletin of the Institute for Mathematics and its Applications. 1990. Vol. 26. No. 1–2. P. 15–17.

Материал поступил в редколлегию 29.03.2011

Адрес автора
ЕМЕЛЬЯНОВ Павел Геннадьевич
Институт систем информатики им. А. П. Ершова СО РАН
пр. Акад. Лаврентьева, 6, Новосибирск, 630090, Россия
Новосибирский государственный университет
ул. Пирогова, 2, Новосибирск, 630090, Россия
e-mail: emelyanov@mmf.nsu.ru