Теорема Абъянкара — Моха — Судзуки

Л. Г. Макар-Лиманов

Эта заметка содержит полное доказательство Теоремы Абъянкара — Моха — Судзуки (AMC-теоремы, см. «Математическое просвещение», вып. 12, задача 11). Доказательство основано на новом алгоритме для нахождения алгебраической зависимости двух многочленов от одной переменной. Для понимания заметки не требуется знаний, выходящих за рамки школьной программы.

§ 1. Введение

AMC-теорема характеризует пары многочленов от одной переменной, через которые можно выразить саму переменную.

Вот её точная формулировка (для рациональных коэффициентов).

Теорема AMC. *Пусть f и g — два многочлена с рациональными коэффициентами степеней n и m от переменной z, и пусть существует такой многочлен Q от двух переменных, что $Q(f, g) = z$. Тогда бóльшая степень делится на меньшую степень без остатка.*

Многочлены с рациональными коэффициентами мы рассматриваем для простоты. Более опытный читатель заметит, что коэффициенты могут быть взяты из любого поля характеристики нуль и даже из поля конечной характеристики.

Интересна история доказательства этой теоремы. Первое доказательство опубликовал в 1956 году известный итальянский математик Беньямино Сегре [1]. Затем в 1970 году появилась работа двух мексиканских математиков Игнасио Канальса и Эмилио Льюиса Риеры [2], указывающая на ошибки в работе Сегре и предлагающая новое доказательство. Наконец, в 1975 году была опубликована статья двух американских математиков Шрирама Шанкара Абъянкара и Тцуонг-Тсиенга Моха [3], в которой и доказательство Сегре, и доказательство Канальса и Льюиса Риеры характеризовались как совершенно ошибочные.

Доказательство Абъянкара и Моха состояло из объёмистой подготовительной статьи, написанной в 1971 году и опубликованной в двух частях

в 1973 году [4], и уже упомянутой основной статьи [3], окончательный вариант которой был написан в 1973 году.

Тем временем молодой японский математик Масакадзу Судзуки, узнав о работе Абъянкара и Моха, написал в 1972 году статью [5], содержащую доказательство. (Это его первая опубликованная статья, появившаяся в печати в 1974 году.) В сноске к статье он упоминает, что ему известно о результате Абъянкара (видимо, он не слышал, что Мох является соавтором), и, оправдывая свою работу, справедливо замечает, что подходы к доказательству совершенно различны. Действительно, его подход — это подход геометра, а подход Абъянкара и Моха чисто алгебраический.

Любопытно, что, упоминая AMC-теорему в своих статьях и выступлениях, Абъянкар зачастую называл её леммой для старшеклассников (high school lemma). После доказательств Абъянкара, Моха и Судзуки появилось не меньше дюжины доказательств AMC-теоремы. Некоторые из них занимают пять-шесть страниц. Правда, чтобы их понять, читатель должен знать намного больше, чем старшеклассник. Автор надеется, что доказательство в этой заметке будет доступно старшеклассникам, интересующимся математикой.

§ 2. Неприводимая зависимость двух многочленов

Возьмём два многочлена f и g от одной переменной z степеней n и m соответственно. Мы хотим проверить, зависимы ли они, т. е. существует ли такой ненулевой многочлен $P(x, y)$ от двух переменных, что $P(f, g) = 0$.

Для натурального числа l рассмотрим все многочлены вида $y^l + R_l$, где $\deg_y(R_l) < l$. Может случиться, что среди них есть многочлен $P(x, y)$, для которого $P(f, g) = 0$, и тогда f и g зависимы. Если $g^l + R_l(f, g)$ не равно нулю для любого R_l, то $\deg_z(g^l + R_l(f, g))$ — натуральное число. (Если $\deg_z(g^l + R_l(f, g)) = 0$ для какого-то $R_l(f, g)$, то $g^l + R_l(f, g)$ — рациональное число и, вычитая его, мы получим многочлен с нулевым значением.) В этом случае выберем тот многочлен Q_l, у которого $\deg_z(Q_l(f, g))$ минимальна. Многочлен Q_l существует, поскольку любое непустое множество натуральных чисел содержит наименьшее число. Обозначим степень этого многочлена через e_l.

Допустим, что $e_a - e_b$ делится на n для некоторых положительных целых чисел a и b и что $a > b$. Тогда $e_a < e_b$. Действительно, если $e_a \geqslant e_b$, то, поскольку $n = \deg(f)$, можно подобрать неотрицательное целое число j и рациональный коэффициент c так, что

$$\deg_y\bigl(Q_a(f, g) - cf^j Q_b(f, g)\bigr) < \deg_z(Q_a(f, g))$$

вопреки определению Q_a.

Теперь мы можем получить противоречие, если для всех l многочлен Q_l определён, т. е. если зависимость вида $y^l + R_l$ не существует. Если поделить целое число на n с остатком, то остаток должен быть одним из чисел $0, 1, \ldots, n-1$. Поэтому все e_l можно распределить по n классам, в каждом из которых остатки e_l при делении на n одинаковы. Поскольку в каждом из этих классов числа убывают с ростом l, каждый класс может содержать лишь конечное число элементов. Поэтому Q_l может существовать только для конечного числа l. Следовательно, для всякого достаточно большого l зависимость вида $y^l + R_l(x, y)$, где $g^l + R_l(f, g) = 0$, существует.

Найдём зависимость Q такого вида с минимальным l. Можно найти, конечно, и зависимость

$$P = p_0(x)y^k + p_1(x)y^{k-1} + \ldots + p_k(x)$$

с минимальной степенью по y, но она может задаваться многочленом, у которого ведущий коэффициент p_0 не равен единице, а является многочленом от x ненулевой степени. Кроме минимальности k мы можем предположить, что коэффициенты p_i не имеют общего делителя, иначе на него можно было бы сократить. На самом деле после сокращения получаем $P = Q$, и мы в этом сейчас убедимся.

Разумеется, k не может быть больше l. Если $k = l$, то $P = p_0 Q$, поскольку $P - p_0 Q$ — тоже зависимость и $\deg_y(P - p_0 Q) < k$. В этом случае $P = Q$, поскольку коэффициенты многочлена P не имеют общего делителя.

Если $l > k$, заменим многочлен Q на $Q_1 = p_0 Q - y^{l-k} P$. Многочлен Q_1 — тоже зависимость между f и g, если $Q_1 \neq 0$. В этом случае степень Q_1 по y не меньше k, поскольку зависимостей меньшей степени не существует. Заменим Q_1 на $Q_2 = p_0 Q_1 - r_1 y^{l_1 - k} P$, где $l_1 = \deg_y(Q_1)$, а многочлен $r_1(x)$ подобран так, чтобы ведущие коэффициенты $p_0 Q_1$ и $r_1 y^{l_1 - k} P$ совпадали. Если результат не нуль, проделаем ещё один шаг, и т. д. По построению $\deg_y(Q_{i+1}) < \deg_y(Q_i)$. Поскольку все Q_i являются зависимостями, через несколько шагов будет получено $Q_j = 0$.

Многочлены Q_i можно выразить через P и Q: $Q_i = s_i(x)Q - S_i(x, y)P$. Следовательно, $0 = Q_j = s_j(x)Q - S_j(x, y)P$ и $s_j(x)Q = S_j(x, y)P$. Если коэффициенты S_j как многочлена от y имеют общий делитель $d(x)$, то, поскольку ведущий коэффициент многочлена Q равен единице, s_j делится на $d(x)$ и на него можно сократить. В результате мы получим $s(x)Q = S(x, y)P$, где общие делители коэффициентов многочленов P, Q и S равны 1.

Многочлен s является произведением ведущих коэффициентов S и P как многочленов от y и поэтому делится на p_0. Если $p_0 = q_1 q_2$, где степени многочленов q_1, q_2 положительны, то мы проверим, разлагаются ли многочлены q_1 и q_2 подобным образом, и продолжим разложение p_0 на мно-

жители с положительными степенями, пока это возможно. Поскольку сумма степеней всех множителей равна степени p_0, процесс разложения остановится и мы получим разложение p_0 в произведение неразложимых далее многочленов. Такие многочлены называются неприводимыми. Это разложение подобно разложению целого числа на простые множители.

Возьмём один из сомножителей этого разложения — многочлен q. Он делит p_0 и может делить и другие коэффициенты p_i. Однако он не может делить все коэффициенты, поскольку их общий делитель — единица. Среди не делящихся коэффициентов выберем коэффициент p_j при наибольшей степени y и поступим аналогично с

$$S = \sum_{i=0}^{r} s_i(x) y^{r-i}$$

— выберем коэффициент s_l, не делящийся на q, при наибольшей возможной степени y.

В произведении P и S рассмотрим коэффициент $\sum_{a+b=j+l} p_a s_b$ при $y^{k+r-j-l}$. Все слагаемые $p_a s_b$, кроме $p_j s_l$, делятся на q, так как либо $j < a$, либо $l < b$ и либо p_a, либо s_b делится на q. Поскольку $SP = sQ$, многочлен $\sum_{a+b=j+l} p_a s_b$ делится на s и тоже должен делиться на q. (Как вы помните, s делится на p_0.) Поэтому $p_j s_l$ тоже делится на q.

Таким образом, произведение двух многочленов от x, не делящихся на неприводимый многочлен q, делится на q. Осталось привести это к противоречию.

Допустим, что такая ситуация возможна, и найдём неприводимый многочлен ρ минимальной степени, для которого это происходит. Для него, в свою очередь, найдём два многочлена τ_1 и τ_2, не делящиеся на него, с делящимся произведением: $\tau_1\tau_2 = \rho\sigma$ и с минимальной возможной суммой степеней. Степени многочленов τ_1, τ_2 меньше $\deg_x(\rho)$, поскольку иначе можно, скажем, τ_1 поделить с остатком на ρ и представить в виде $\tau_1 = \alpha\rho + \tau_3$, где $\deg_x(\tau_3) < \deg_x(\rho)$. Но тогда ρ делит $\tau_3\tau_2$, поскольку

$$\rho\sigma = \tau_1\tau_2 = (\alpha\rho + \tau_3)\tau_2 = \alpha\rho\tau_2 + \tau_3\tau_2.$$

Многочлен σ имеет положительную степень, так как иначе $\rho = (\sigma^{-1}\tau_1)\tau_2$, а ρ — неприводимый многочлен, и

$$\deg_x(\sigma) = \deg_x(\tau_1\tau_2) - \deg_x(\rho) < \deg_x(\rho).$$

Разложим многочлен σ на неприводимые множители так же, как мы разложили многочлен p_0. Возьмём один из этих множителей σ_1. Поскольку

$\deg_x(\sigma_1) < \deg_x(\rho)$, либо τ_1, либо τ_2 делится на многочлен σ_1 и его можно сократить в равенстве $\rho\sigma = \tau_1\tau_2$. Это и приводит нас к противоречию: сумма степеней многочленов τ_1, τ_2 не была минимальной.

Итак, мы убедились, что многочлен p_0 должен иметь нулевую степень и потому существует минимальная зависимость

$$P = y^k + p_1(x)y^{k-1} + \ldots + p_k(x)$$

многочленов f и g с ведущим коэффициентом 1. Понятно, что любая зависимость получается из минимальной умножением на многочлен от x и y.

В следующем параграфе мы научимся её находить.

§ 3. Алгоритм для нахождения зависимости

Вначале неформально опишем процедуру получения многочлена P.

Найдём минимальное a, для которого степень g^a делится на степень f, а затем многочлен $g^a - cf^b$, где рациональное число c и неотрицательное целое число b подобраны так, что $\deg_z(g^a - cf^b) < \deg_z(g^a)$. Затем, если существует такой моном f^ig^j, что $\deg_z(f^ig^j) = \deg_z(g^a - cf^b)$, возьмём $g^a - cf^b - c_1f^ig^j$, где рациональное число c_1 подобрано так, что

$$\deg_z(g^a - cf^b - c_1f^ig^j) < \deg_z(g^a - cf^b).$$

Уменьшим степень результата, если найдётся подходящий моном, и так до тех пор, пока не получим многочлен h, степень которого не может быть уменьшена.

Если $h = 0$, мы получили зависимость. Если $h \neq 0$, найдём минимальное a', при котором для $h^{a'}$ существует моном f^ig^j с такой же степенью, как у $h^{a'}$. Затем уменьшим эту степень, вычтя cf^ig^j из $h^{a'}$. Продолжим уменьшение степени, вычитая мономы от f, g и h, пока не получим многочлен h', степень которого не может быть уменьшена, и т. д. После нескольких таких шагов мы получим зависимость.

Посмотрим, как это работает, на примере $f = z^4$, $g = z^6 - z$. Нужно начать с $g^2 - f^3 = -2z^7 + z^2$, так что $h = -2z^7 + z^2$. Далее получаем $h^2 - 4f^2g = z^4$, $h^2 - 4f^2g - f = 0$, так что $h^2 - 4f^2g - f = (g^2 - f^3)^2 - 4f^2g - f$ — это зависимость, которую мы ищем.

Дадим теперь формальное описание алгоритма.

Формальное описание

Первый шаг. Положим $g_0 = g$, $m_0 = \deg_z(g_0)$, $n = \deg_z(f)$. Найдём наибольший общий делитель d_0 чисел n и m_0. Затем найдём $a_0 = n/d_0$, $b_0 = m_0/d_0$.

Тогда $\deg_z(g_0^{a_0}) = \deg_z(f^{b_0})$ и a_0 — минимальное положительное число, для которого $\deg_z(g_0^{a_0})$ делится на n. Найдём $k_0 \in \mathbb{Q}$, для которого $m_{0,1} = \deg_z(g_0^{a_0} - k_0 f^{b_0}) < \deg_z(g_0^{a_0})$. Если $m_{0,1}$ делится на d_0, найдём моном $f^i g_0^{j_0}$ (где $i, j_0 \in \mathbb{Z}$, $0 \leqslant j_0 < a_0$), для которого $\deg_z(f^i g_0^{j_0}) = m_{0,1}$, а также $k_1 \in \mathbb{Q}$, для которого $m_{0,2} = \deg_z(g_0^{a_0} - k_0 f^{b_0} - k_1 f^i g_0^{j_0}) < m_{0,1}$, и т. д.

Если после конечного числа уменьшений степени мы получим нуль, зависимость получена и мы останавливаем алгоритм.

Если после конечного числа уменьшений степени мы получим $m_{0,i}$, не делящееся на d_0, обозначим соответствующий многочлен g_1 и перейдём к следующему шагу.

Как показано ниже, алгоритм всегда останавливается после конечного числа шагов.

Общий шаг. Допустим, что после s шагов мы получили $g_0, \ldots, g_s$. Положим $m_i = \deg_z(g_i)$. Найдём наибольший общий делитель d_i чисел $n, m_0, \ldots, m_i$. Число d_i положительно, хотя про числа m_i это не ясно. Положим $d_{-1} = n$ и $a_i = d_{i-1}/d_i$ для $0 \leqslant i \leqslant s$. (Легко видеть, что $a_s m_s$ делится на d_{s-1} и что a_s — наименьшее положительное число, обладающее этим свойством.) Моном $\mathbf{m} = f^i g_0^{j_0} \ldots g_s^{j_s}$, где $i, j_0, \ldots, j_s \in \mathbb{Z}$ и $0 \leqslant j_k < a_k$ при $k = 0, \ldots, s$, назовём *s-стандартным*. Найдём $(s-1)$-стандартный моном $\mathbf{m}_{s,0}$, у которого $\deg_z(\mathbf{m}_{s,0}) = a_s m_s$, а также найдём $c_0 \in \mathbb{Q}$, для которого $m_{s,1} = \deg_z(g_s^{a_s} - c_0 \mathbf{m}_{s,0}) < a_s m_s$. Если $m_{s,1}$ делится на d_s, найдём s-стандартный моном $\mathbf{m}_{s,1}$, у которого $\deg_z(\mathbf{m}_{s,1}) = m_{s,1}$, а также найдём $c_1 \in \mathbb{Q}$, для которого $m_{s,2} = \deg_z(g_s^{a_s} - c_0 \mathbf{m}_{s,0} - c_1 \mathbf{m}_{s,1}) < m_{s,1}$, и т. д. (Мы проверим в лемме 1, что любое число, делящееся на d_s, является степенью s-стандартного монома.)

Если после конечного числа уменьшений степени мы получим нуль, зависимость получена и мы останавливаем алгоритм.

Если после конечного числа уменьшений степени мы получим $m_{s,i}$, не делящееся на d_s, обозначим соответствующий многочлен g_{s+1} и перейдём к следующему шагу.

Как показано ниже, алгоритм всегда останавливается после конечного числа шагов.

Замечание. Если g_{i+1} найдено, то $d_{i+1} = (d_i, m_{i+1}) < d_i$, поскольку m_{i+1} не делится на d_i; следовательно, $d_0 > d_1 > \ldots > d_s$.

Если алгоритм нашёл g_i, то g_i — это многочлен от f, g и, возможно, от f^{-1}, поскольку мы пока не знаем, что стандартные мономы не содержат отрицательных степеней f. (В случае поля рациональных чисел и любого поля характеристики нуль отрицательные степени не появляются и мы это докажем.)

Для выражений вида $h = \sum_{i=0}^{k} g_i g^i$, $k \geqslant 0$, где $g_i = \sum_{j=-a}^{b} f^j$, $a \geqslant 0$, $b \geqslant 0$, мы будем использовать следующие четыре функции. Во-первых, степени $\deg_f(h)$, $\deg_g(h)$ относительно f и g, причём $\deg_f(h)$ может оказаться отрицательной, и степень $\deg_z(h)$ относительно z (выражение $h(f(z), g(z))$ можно записать как $\dfrac{h_0(f(z), g(z))}{h_1(f(z), g(z))}$, где h_0 и h_1 являются многочленами,

$$\deg_z(h) = \deg_z(h_0(f(z), g(z)) - \deg_z(h_1(f(z), g(z))).$$

Эти три функции обладают обычными свойствами степени. Четвёртая функция, pow_f, определена только для стандартных мономов:

$$\mathrm{pow}_f(f^i g_0^{j_0} \dots g_s^{j_s}) = i.$$

Эта функция не является степенной, поскольку произведение двух стандартных мономов может не быть стандартным мономом: например, степень g_0 может стать слишком большой в произведении.

Выражения вида $\sum_{j=-a}^{b} f_j f^j$, $a \geqslant 0$, $b \geqslant 0$, $f_j \in \mathbb{Q}$, называются многочленами Лорана. Таким образом, h — это многочлен от g с коэффициентами — многочленами Лорана от f.

Лемма 1. *Если элементы $g_0, g_1, \dots, g_s$ определены, то*:

(а) *для любого $a \in \mathbb{Z}$, делящегося на $d_s = (n, m_0, \dots, m_s)$, существует единственный s-стандартный моном $\mathbf{m}$, у которого $\deg_z(\mathbf{m}) = a$*;

(б) *для $t \leqslant s$ имеем $\deg_g(g_t) = \prod_{i=0}^{t-1} a_i$ и g_t является многочленом от g с ведущим коэффициентом единица*;

(в) *для любого целого неотрицательного числа $d < a_s \deg_g(g_s)$ существует единственный s-стандартный моном $\mathbf{m}$, у которого $\deg_g(\mathbf{m}) = d$, $\mathrm{pow}_f(\mathbf{m}) = 0$.*

Доказательство. В этом доказательстве мы дважды используем так называемый принцип Дирихле: если есть два конечных множества A и B с одинаковым количеством элементов ($|A| = |B|$) и функция из A в B (определённая на всём A), отображающая разные элементы A в разные элементы B, то в каждый элемент B отображён какой-то элемент A.

(а) Если $\deg_z(\mu) - \deg_z(\nu)$ делится на n и $\mathrm{pow}_f(\mu) = \mathrm{pow}_f(\nu) = 0$ для s-стандартных мономов $\mu = g_0^{j_0} \dots g_s^{j_s}$ и $\nu = g_0^{i_0} \dots g_s^{i_s}$, то $\mu = \nu$. Действительно, если $\sum_{k=0}^{s} j_k m_k - \sum_{k=0}^{s} i_k m_k$ делится на n, то $j_s m_s - i_s m_s$ делится на d_{s-1} (поскольку $n = \deg_z(f)$, а d_{s-1} — наибольший общий делитель $n, m_0, \dots, m_{s-1}$). Таким образом, $(j_s - i_s)m_s$ делится на d_{s-1}, в то время как $-a_s < j_s - i_s < a_s$, поскольку $0 \leqslant i_s, j_s < a_s$. Поэтому $j_s - i_s = 0$, так как по определению a_s — наименьшее целое положительное число, для которого

$a_s m_s$ делится на d_{s-1}. Значит, $j_s = i_s$, и мы можем аналогично проверить, что $j_{s-1} = i_{s-1}$, $j_{s-2} = i_{s-2}$, $\ldots$, $j_0 = i_0$.

Имеется в точности

$$\prod_{k=0}^{s} a_k = \frac{d_{-1}}{d_s} = \frac{n}{d_s}$$

различных s-стандартных мономов μ_i, у которых $\mathrm{pow}_f(\mu_i) = 0$. Их степени по z дают, как только что доказано, разные остатки при делении на n и делятся на d_s. Поскольку таких остатков тоже n/d_s, по принципу Дирихле для любого такого остатка найдётся соответствующий моном. Поэтому для любого целого числа l, делящегося на d_s, найдётся ровно один такой s-стандартный моном μ, $\mathrm{pow}_f(\mu) = 0$, что n делит $l - \deg_z(\mu)$. Домножив его на f в подходящей степени, найдём единственный s-стандартный моном ν, для которого $\deg_z(\nu) = l$.

(б) Проверим по индукции, что $\deg_g(g_t) = \prod_{i=0}^{t-1} a_i$ и что g_t — многочлен от g с ведущим коэффициентом единица. База индукции очевидна, поскольку $g_0 = g$. Предположим, что $\deg_g(g_k) = \prod_{i=0}^{k-1} a_i$ для всех $k < t+1$. Тогда у t-стандартного монома $\mathbf{m} = g_0^{j_0} \ldots g_t^{j_t}$ степень равна

$$\begin{aligned}\deg_g(\mathbf{m}) &= \sum_{l=0}^{t} j_l \deg_g(g_l) \leqslant \sum_{l=0}^{t} (a_l - 1) \deg_g(g_l) = \\ &= \sum_{l=0}^{t-1} (\deg_g(g_{l+1}) - \deg_g(g_l)) + (a_t - 1)\deg_g(g_t) = \\ &= \deg_g(g_t) - 1 + (a_t - 1)\deg_g(g_t) = a_t \deg_g(g_t) - 1.\end{aligned}$$

Следовательно, $\deg_g(\mathbf{m}) \leqslant a_t \deg_g(g_t) - 1$. По определению

$$g_{t+1} = g_t^{a_t} - r_t(f, g_0, \ldots, g_t).$$

Поскольку все мономы из r_t являются t-стандартными,

$$\deg_g(r_t) \leqslant a_t \deg_g(g_t) - 1$$

и g_{t+1} — многочлен степени

$$\deg_g(g_{t+1}) = \deg_g(g_t^{a_t}) = a_t \prod_{i=0}^{t-1} a_i = \prod_{i=0}^{t} a_i$$

с ведущим коэффициентом единица.

(в) Если $\deg_g(\mu) = \deg_g(\nu)$ и $\mathrm{pow}_f(\mu) = \mathrm{pow}_f(\nu)$ для s-стандартных мономов μ и ν, то $\mu = \nu$. Действительно,

$$\deg_g(\mu) = \sum_{k=0}^{s} j_k \deg_g(g_k), \quad \deg_g(\nu) = \sum_{k=0}^{s} i_k \deg_g(g_k).$$

В каждой сумме все слагаемые, кроме i_0 и j_0, заведомо делятся на a_0. Из $\deg_g(\mu) = \deg_g(\nu)$ следует, что $j_0 - i_0$ делится на a_0, откуда $j_0 = i_0$, поскольку $0 \leqslant j_0 < a_0$ и $0 \leqslant i_0 < a_0$. После этого мы можем доказать, что $j_1 = i_1$, поскольку $j_0 = i_0$ влечёт делимость $j_1 - i_1$ на a_1, и т. д.

Есть в точности $\prod_{k=0}^{s} a_k = a_s \deg_g(g_s)$ различных s-стандартных мономов μ_i, у которых $\mathrm{pow}_f(\mu_i) = 0$. Как мы убедились в п. (б), ровно столько же есть возможностей для степеней s-стандартных мономов по g, поскольку для s-стандартного монома $\deg_g(\mu) < a_s \deg_g(g_s)$. Поэтому по принципу Дирихле для любого d, удовлетворяющего условию $0 \leqslant d < a_s \deg_g(g_s)$, существует единственный s-стандартный моном $\mathbf{m}$, у которого $\deg_g(\mathbf{m}) = d$, $\mathrm{pow}_f(\mathbf{m}) = 0$. □

Замечание. Таким образом, стандартный моном $\mathbf{m} = f^i g_0^{j_0} \dots g_s^{j_s}$ полностью определяется величинами $i = \mathrm{pow}_f(\mathbf{m})$ и $\deg_g(\mathbf{m})$.

Лемма 2. *На каждом шаге алгоритм останавливается после конечного числа уменьшений степени.*

Доказательство. Во втором параграфе мы убедились в том, что существует неприводимая зависимость между f и g, заданная многочленом P степени k по g, у которого ведущий коэффициент — единица. Допустим, что $k < a_s \deg_g(g_s)$. Тогда P можно выразить суммой стандартных s-мономов, у которых $\mathrm{pow}_f = 0$, с коэффициентами — многочленами Лорана. Действительно, согласно лемме 1 для любого целого неотрицательного числа $d < a_s \deg_g(g_s)$ существует единственный s-стандартный моном $\mathbf{m}$, у которого $\deg_g(\mathbf{m}) = d$, $\mathrm{pow}_f(\mathbf{m}) = 0$ (пункт (в)), а согласно пункту (б) его ведущий коэффициент — единица. Найдём стандартный моном $\mathbf{m_1}$, $\mathrm{pow}_f(\mathbf{m_1}) = 0$, имеющий степень k по g. Тогда $\deg_g(P(f,g) - \mathbf{m_1}) < k$ и $P(f,g) - \mathbf{m_1}$ — многочлен от g с коэффициентами — многочленами Лорана от f. Найдём теперь стандартный моном $\mathbf{m_2}$, $\mathrm{pow}_f(\mathbf{m_2}) = 0$, для которого $\deg_g(\mathbf{m_2}) = \deg_g(P(f,g) - \mathbf{m_1})$, и такой многочлен Лорана c_2 от f, что $\deg_g(P(f,g) - \mathbf{m_1} - c_2\mathbf{m_2}) < \deg_g(P(f,g) - \mathbf{m_1})$. Продолжим понижение степени, вычитая соответствующие стандартные мономы, имеющие $\mathrm{pow}_f = 0$, с коэффициентами — многочленами Лорана от f. В конце мы получим многочлен нулевой степени, являющийся многочленом Лорана. Поскольку 1 — тоже стандартный моном, мы получим обещанное

представление $P=\sum_i c_i\mathbf{m_i}$. Но тогда $P(f,g)\neq 0$, поскольку по лемме 1(а) величины $\deg_z(\mathbf{m_i})$ дают различные остатки при делении на $n=\deg_z(f)$. Поэтому различные слагаемые $c_i\mathbf{m_i}$ имеют разные степени по z и их сумма не может быть нулём. Следовательно, $k\geqslant a_s\deg_g(g_s)$.

Если $k=a_s\deg_g(g_s)$, то $\deg_g(P-g_s^{a_s})<k$ и $P-g_s^{a_s}=\sum_i(c_i\mathbf{m_i})$. В этом случае алгоритм выдаст нуль.

Если $k>a_s\deg_g(g_s)$, рассмотрим выражения вида $c_0g_s^{a_s}-\sum_i c_i\mathbf{m_i}$, где c_i — многочлены от f, подобранные так, что $c_0g_s^{a_s}-\sum_i c_i\mathbf{m_i}$ принадлежат $\mathbb{Q}[f,g]$, т. е. не содержат отрицательных степеней f. Назовём такие выражения допустимыми. Поскольку k — это степень минимальной зависимости, $\deg_z(c_0g_s^{a_s}-\sum_i c_i\mathbf{m_i})\neq 0$, если хотя бы один из многочленов c_i ненулевой.

Предположим, что $\deg_z(c_0g_s^{a_s}-\sum_i c_i\mathbf{m_i})$ делится на d_s для всех допустимых выражений. Тогда рассуждение, похожее на рассуждение во втором параграфе, показывает, что некоторое допустимое выражение является зависимостью между f и g, что невозможно, поскольку $k>a_s\deg_g(g_s)$.

Действительно, все допустимые выражения можно распределить по n/d_s классам в соответствии с остатком при делении степени на n. При доказательстве леммы 1(а) мы убедились, что для каждого такого остатка найдётся соответствующий s-стандартный моном μ_i с $\mathrm{pow}_f(\mu_i)=0$. Значит, в каждом классе найдётся s-стандартный моном ν_i, являющийся допустимым выражением. Для определённости мы можем считать, что величина $\mathrm{pow}_f(\nu_i)$ минимальная из возможных.

Обозначим через Md_s максимальную степень элементов ν_i по z. Пусть Q — произвольное допустимое выражение. Вычитая из Q элементы вида $qf^j\nu_i$, $q\in\mathbb{Q}$, $j\in\mathbb{N}$, мы получим элемент $\delta(Q)=Q-r_l$ (где r_l — сумма s-стандартных мономов) со степенью по z, меньшей чем Md_s.

Степени многочленов $\delta(Q)$ распределены по M классам: $\{\deg_z(\delta(Q))=$ $=d_s,2d_s,\ldots,Md_s\}$ (некоторые из них могут оказаться пустыми). В каждом непустом классе выберем некоторый элемент $\delta(Q_i)$. Тогда любой $\delta(Q)$ имеет вид $\delta(Q)=\sum_i q_i\delta(Q_i)$ для некоторых рациональных чисел $q_0,\ldots,q_{M-1}$. Действительно, $\deg_z(\delta(Q))=\deg_z(\delta(Q_i))$ для одного из выбранных представителей, и можно подобрать $q_i\in\mathbb{Q}$ так, что

$$\deg_z(\delta(Q)-q_i\delta(Q_i))<\deg_z(\delta(Q)).$$

Поскольку $\deg_z(\delta(Q)-q_i\delta(Q_i))<Md_s$, это число тоже принадлежит одному из классов и процесс можно продолжить, пока степень не станет нулём. Это означает, что $\delta(Q)-q_i\delta(Q_i)=q_0\in\mathbb{Q}$ и $\delta(Q)=\sum_{i=0}^{M-1}q_i\delta(Q_i)$, где $\delta(Q_0)=1$.

Рассмотрим теперь допустимое выражение $f^lg_s^{a_s}$, где l больше максимума $\deg_f(\delta(Q_i))$. Поскольку слагаемые в r_l являются s-стандартными мономами, их степени по g меньше, чем $a_s\deg_g(g_s)$. Поэтому в $\delta(f^lg_s^{a_s})$ как

многочлене от f, g сохранится моном $f^l g^{a_s \deg_g(g_s)}$, содержавшийся в $f^l g_s^{a_s}$, и степень $\delta(f^l g_s^{a_s})$ по f не может быть меньше l. Как мы видели выше, $\delta(f^l g_s^{a_s}) = \sum_{i=0}^{M-1} q_i \delta(Q_i)$ для некоторых $q_0, \ldots, q_{M-1} \in \mathbb{Q}$ (хотя степень левой части по f больше степени правой части по f, они имеют одинаковую степень как многочлены от z). Но тогда многочлен $\delta(f^l g_s^{a_s}) - \sum_{i=0}^{M-1} q_i \delta(Q_i)$ является зависимостью между f и g, у которой степень по g меньше k, что невозможно.

Полученное противоречие показывает, что $\deg(c_0 g_s^{a_s} - \sum_i c_i \mathbf{m_i})$ не делится на d_s при некотором выборе $c_i \in \mathbb{Q}[f]$. Как мы увидим, в этом случае алгоритм даёт g_{s+1}.

Найдём $\delta = c_0 g_s^{a_s} - \sum_i c_i \mathbf{m_i}$, для которого $\deg_z(\delta)$ не делится на d_s. Если $c_0 = q_0 f^l$, то, поделив на c_0, мы получим

$$g_s^{a_s} - \sum_i \frac{c_i}{q_0 f^l} \mathbf{m_i} = \frac{\delta}{q_0 f^l},$$

где все $\frac{c_i}{q_0 f^l}$ — многочлены Лорана. Запишем каждое слагаемое $\frac{c_i}{q_0 f^l} \mathbf{m_i}$ в виде $\alpha_{i,1} + \alpha_{i,2}$, где степень по z стандартных мономов в $\alpha_{i,1}$ больше $\deg_z\Big(\frac{\delta}{q_0 f^l}\Big)$, а в $\alpha_{i,2}$ меньше. (Равенство невозможно, поскольку $\deg_z(\delta)$ не делится на d_s.) Тогда

$$g_s^{a_s} - \sum_i \alpha_{i,1} = \frac{\delta}{q_0 f^l} + \sum_i \alpha_{i,2} \quad \text{и} \quad g_{s+1} = g_s^{a_s} - \sum_i \alpha_{i,1},$$

где $\deg_z(g_{s+1}) = \deg_z\Big(\frac{\delta}{q_0 f^l}\Big)$ не делится на d_s. Действительно, степени по z стандартных мономов попарно различны (лемма 1(a)). Поэтому $\sum_i \alpha_{i,1}$ содержит именно те стандартные мономы, которые будут использованы в алгоритме для уменьшения степени $g_s^{a_s}$.

Если $c_0 = q_0 f^l - r$, где $\deg_f(r) < l$, рассмотрим

$$\frac{c_0}{q_0 f^l} g_s^{a_s} - \sum_{i=1} \frac{c_i}{q_0 f^l} \mathbf{m_i} = \frac{\delta}{q_0 f^l}.$$

В левой части коэффициенты являются многочленами Лорана, а

$$\frac{c_0}{q_0 f^l} = 1 - w,$$

где $\deg_f(w) \leqslant -1$. Воспользовавшись формулой

$$\frac{1}{1-w} = 1 + w + \ldots + w^a + \frac{w^{a+1}}{1-w},$$

мы получим

$$g_s^{a_s} - \Big(1 + w + \ldots + w^a + \frac{w^{a+1}}{1-w}\Big) \sum_i \frac{c_i}{q_0 f^l} \mathbf{m_i} = \frac{\delta}{q_0 f^l (1-w)}$$

и

$$g_s^{a_s} - (1 + w + \ldots + w^a) \sum_i \frac{c_i}{q_0 f^l} \mathbf{m_i} = \frac{\delta}{q_0 f^l (1-w)} + \frac{w^{a+1}}{1-w} \sum_i \frac{c_i}{q_0 f^l} \mathbf{m_i}.$$

Поскольку $\deg_z(w) \leqslant -n$, при достаточно большом a получим

$$\deg_z\Big(\frac{w^{a+1}}{1-w} \sum_i \frac{c_i}{q_0 f^l} \mathbf{m_i}\Big) < \deg_z\Big(\frac{\delta}{q_0 f^l}\Big).$$

Как и в случае $c_0 = q_0 f^l$, положим

$$(1 + w + \ldots + w^a) \frac{c_i}{q_0 f^l} \mathbf{m_i} = \alpha_{i,1} + \alpha_{i,2},$$

где степень по z стандартных мономов в $\alpha_{i,1}$ больше $\deg_z\Big(\frac{\delta}{q_0 f^l}\Big)$, а в $\alpha_{i,2}$ меньше. Тогда

$$g_{s+1} = g_s^{a_s} - \sum_i \alpha_{i,1},$$

где $\deg_z(g_{s+1}) = \deg_z\Big(\frac{\delta}{q_0 f^l}\Big)$ не делится на d_s. □

Мы доказали, что алгоритм работает. Осталось проверить, что после конечного числа шагов он выдаст неприводимую зависимость.

Лемма 3. *После конечного числа шагов алгоритм выдаст нуль и неприводимую зависимость между $f(z)$ и $g(z)$.*

Доказательство. Как было замечено выше, $d_0 > d_1 > \ldots > d_i$. Поскольку $d_i \in \mathbb{N}$, через конечное число шагов мы получим минимальное d_s, и после этого алгоритм выдаст $0 = g_s^{a_s}(f, g) - r_s(f, g)$. В доказательстве леммы 2 было показано, что $\deg_y(P) = a_s \deg_g(g_s)$. Следовательно, $P = g_s^{a_s}(x, y) - r_s(x, y)$. □

§ 4. Доказательство теоремы AMC

Ещё одна лемма — и мы сможем доказать теорему AMC.

Лемма 4. *Все g_i являются многочленами от f и g.*

Доказательство. Упорядочим мономы $f^i g^j$, $i, j \in \mathbb{Z}$, лексикографически по степеням $\deg_g$, $\deg_f$, т. е. будем говорить, что $f^{i_1} g^{j_1} > f^{i_2} g^{j_2}$, если $j_1 > j_2$ или $j_1 = j_2$, $i_1 > i_2$.

Назовём моном *отрицательным*, если его степень по f отрицательна, в противном случае назовём его *положительным*.

Обозначим через L множество многочленов от g с коэффициентами — многочленами Лорана от f, т. е. $L = \mathbb{Q}[g, f, f^{-1}]$. Введём для элемента $h \in L$ функцию gap следующим образом. Если $h \notin \mathbb{Q}[f, g]$, то $\operatorname{gap}(h)$ — это моном $\overline{h} \div \widetilde{h}$ (здесь $a \div b = a/b$), где $\overline{h}$ — самый большой моном в h, а $\widetilde{h}$ — самый большой отрицательный моном в h; если $h \in \mathbb{Q}[f, g]$, то $\operatorname{gap}(h) = \infty$, где ∞ больше любого монома по определению.

Будем пользоваться следующими легко проверяемыми свойствами функции gap:

(а) $\operatorname{gap}(h_1 h_2) \geqslant \min(\operatorname{gap}(h_1), \operatorname{gap}(h_2))$;

(б) $\operatorname{gap}(h^d) = \operatorname{gap}(h)$, $d \in \mathbb{N}$, если у h как многочлена от g ведущий коэффициент — единица.

Так как g_{s+1} — это элемент, полученный на последнем шаге алгоритма, т. е. g_{s+1} — неприводимая зависимость между $f(z)$ и $g(z)$, мы знаем, что $\operatorname{gap}(g_{s+1}) = \infty$, поскольку g_{s+1} — многочлен от f и g. Мы собираемся проверить, что $\operatorname{gap}(g_{j+1}) \leqslant \operatorname{gap}(g_j)$, где g_j, $j = 0, 1, \ldots, s+1$, рассматриваются как элементы L. Из этого будет следовать, что $\operatorname{gap}(g_j) = \infty$ для $j = 0, 1, \ldots, s$. Поскольку $\operatorname{gap}(h) = \infty$ означает, что $h \in K[f, g]$, лемма будет доказана.

Воспользуемся индукцией. Поскольку $\operatorname{gap}(g_1) \leqslant \operatorname{gap}(g_0) = \infty$, база индукции очевидна.

Предположим, что $\operatorname{gap}(g_{j+1}) \leqslant \operatorname{gap}(g_j)$, если $j < k$. Имеем $g_{k+1} = g_k^{a_k} - r_k$ и $\operatorname{gap}(g_k^{a_k}) = \operatorname{gap}(g_k)$ по свойству (б) (по лемме 1(б) у всех g_i ведущий коэффициент — единица). Чтобы доказать, что $\operatorname{gap}(g_{k+1}) \leqslant \operatorname{gap}(g_k)$, достаточно проверить, что самые большие отрицательные мономы у r_k и $g_k^{a_k}$ различны. Действительно, пусть ϱ — самый большой отрицательный моном r_k, а γ — самый большой отрицательный моном $g_k^{a_k}$ и они не равны. Если $\gamma > \varrho$, то $\operatorname{gap}(g_{k+1}) = g^{a_0 \cdots a_k} \div \gamma = \operatorname{gap}(g_k^{a_k}) = \operatorname{gap}(g_k)$, а если $\varrho > \gamma$, то $\operatorname{gap}(g_{k+1}) = g^{a_0 \cdots a_k} \div \varrho < \operatorname{gap}(g_k^{a_k}) = \operatorname{gap}(g_k)$.

Если $g_k^{a_k}$ не содержит отрицательных мономов, то g_k — многочлен и $\operatorname{gap}(g_{k+1}) \leqslant \operatorname{gap}(g_k) = \infty$, а если r_k не содержит отрицательных мономов, то $\operatorname{gap}(g_{k+1}) = \operatorname{gap}(g_k)$.

Вспомним, что r_k является суммой k-стандартных мономов с рациональными коэффициентами. Эти мономы тоже можно лексикографически упорядочить по $\deg_g$, pow_f (а именно, $\mathbf{m_i} > \mathbf{m_j}$, если $\deg_g(\mathbf{m_i}) > \deg_g(\mathbf{m_j})$ или если $\deg_g(\mathbf{m_i}) = \deg_g(\mathbf{m_j})$ и $\operatorname{pow}_f(\mathbf{m_i}) > \operatorname{pow}_f(\mathbf{m_j})$). Стандартный моном $\mathbf{m}$ является элементом в L. Легко видеть, что самый большой его моном — это $\overline{\mathbf{m}} = f^i g^j$, где $i = \operatorname{pow}_f(\mathbf{m})$, а $j = \deg_g(\mathbf{m})$. Таким образом, $\mathbf{m_i} < \mathbf{m_j}$, если $\overline{\mathbf{m_i}} < \overline{\mathbf{m_j}}$. Два различных стандартных монома не могут оказаться равными относительно введённого порядка, поскольку $i = \operatorname{pow}_f(\mathbf{m})$ и $j = \deg_g(\mathbf{m})$

определяют стандартный моном однозначно (см. замечание к лемме 1). Назовём k-стандартный моном $\mathbf{m}$ *отрицательным*, если $\mathrm{pow}_f(\mathbf{m}) < 0$, а при $\mathrm{pow}_f(\mathbf{m}) \geqslant 0$ — *положительным*.

Если k-стандартный моном $\mathbf{m}$ отрицателен, то $\mathrm{gap}(\mathbf{m}) = 1$, поскольку его наибольший моном отрицателен. Если $\mathbf{m} = f^i g_0^{j_0} \dots g_k^{j_k}$ положителен, т. е. если $i \geqslant 0$, то

$$\mathrm{gap}(\mathbf{m}) \geqslant \min\bigl(\mathrm{gap}(f^i), \mathrm{gap}(g_0^{j_0}), \dots, \mathrm{gap}(g_k^{j_k})\bigr)$$

по свойству (а),

$$\min\bigl(\mathrm{gap}(f^i), \mathrm{gap}(g_0^{j_0}), \dots, \mathrm{gap}(g_k^{j_k})\bigr) = \min\bigl(\infty, \mathrm{gap}(g_0), \dots, \mathrm{gap}(g_k)\bigr)$$

по свойству (б),

$$\min\bigl(\infty, \mathrm{gap}(g_0), \dots, \mathrm{gap}(g_k)\bigr) = \mathrm{gap}(g_k)$$

по предположению индукции.

Следовательно,

$$\mathrm{gap}(\mathbf{m}) \geqslant \mathrm{gap}(g_k) = \mathrm{gap}(g_k^{a_k}).$$

Поскольку $\deg_g(\mathbf{m}) < \deg_g(g_k^{a_k})$ по лемме 1(б), а $\mathrm{gap}(\mathbf{m}) \geqslant \mathrm{gap}(g_k^{a_k})$, даже если положительный k-стандартный моном $\mathbf{m} \in L$ не является многочленом, его отрицательные мономы меньше, чем наибольший отрицательный моном γ элемента $g_k^{a_k}$. Поэтому только один из отрицательных k-стандартных мономов r_k может иметь наибольший моном равным γ.

Чтобы облегчить понимание доказательства, рассмотрим два случая: (i) $\mathrm{gap}(g_k) < \mathrm{gap}(g_{k-1})$ и (ii) $\mathrm{gap}(g_k) = \mathrm{gap}(g_{k-1})$.

(i) $\mathrm{gap}(g_k) < \mathrm{gap}(g_{k-1})$. Поскольку $g_k = g_{k-1}^{a_{k-1}} - r_{k-1}$ и

$$\mathrm{gap}(g_{k-1}^{a_{k-1}}) = \mathrm{gap}(g_{k-1}) > \mathrm{gap}(g_k),$$

наибольший отрицательный моном ν_{k-1} в r_{k-1} больше, чем наибольший отрицательный моном в $g_{k-1}^{a_{k-1}}$. Отсюда $\mathrm{gap}(g_k) = \overline{g_{k-1}^{a_{k-1}}} \div \overline{\nu_{k-1}}$.

Далее,

$$g_k^{a_k} = (g_{k-1}^{a_{k-1}} - r_{k-1})^{a_k} = g_{k-1}^{a_{k-1}a_k} - R.$$

Поскольку $\deg_g(R) < a_k \deg_g(g_k)$, мы знаем, что R можно представить суммой k-стандартных мономов (лемма 1(в)). Наибольший отрицательный k-стандартный моном μ, являющийся слагаемым в $g_k^{a_k}$, — это наибольший отрицательный k-стандартный моном в R, и он равен $\nu_{k-1} g_k^{a_k - 1}$. Действительно,

$$\mathrm{gap}(g_k^{a_k}) = \mathrm{gap}(g_{k-1}^{a_{k-1}a_k} - R) = \mathrm{gap}(g_k) < \mathrm{gap}(g_{k-1}^{a_{k-1}a_k}) = \mathrm{gap}(g_{k-1});$$

следовательно, наибольший отрицательный моном в $g_{k-1}^{a_{k-1}a_k}$ меньше, чем μ. Более того,

$$\operatorname{gap}(g_k) = \overline{g_{k-1}^{a_{k-1}}} \div \overline{\nu_{k-1}} = \operatorname{gap}(g_k^{a_k}) = \operatorname{gap}(g_{k-1}^{a_{k-1}a_k} - R) = \overline{g_{k-1}^{a_{k-1}a_k}} \div \bar{\mu}.$$

Поскольку $\overline{g_{k-1}^{a_{k-1}}} = \overline{g_k}$, мы получаем, что $\bar{\mu} = \overline{\nu_{k-1}}\overline{g_k^{a_k-1}}$ и k-стандартный моном μ равен $\nu_{k-1}g_k^{a_k-1}$.

Согласно процедуре алгоритма $g_k = g_{k-1}^{a_{k-1}} - r_{k-1}$ и степень по z любого $(k-1)$-стандартного монома в r_{k-1} больше, чем $\deg_z(g_k) = m_k$. Следовательно,

$$\deg_z(\mu) = \deg_z(\nu_{k-1}g_k^{a_k-1}) = \deg_z(\nu_{k-1}) + (a_k - 1)m_k > a_k m_k.$$

Аналогично $g_{k+1} = g_k^{a_k} - r_k$, где степень по z любого k-стандартного монома в r_k не превосходит $a_k m_k$. Следовательно, μ не может быть слагаемым в r_k и наибольшие отрицательные мономы в r_k и $g_k^{a_k}$ различны. Как отмечено перед п. (i), отсюда следует утверждение леммы.

(ii) $\operatorname{gap}(g_k) = \operatorname{gap}(g_{k-1})$. Если $\operatorname{gap}(g_k) = \infty$, то $\operatorname{gap}(g_{k+1}) \leqslant \operatorname{gap}(g_k)$. Поэтому предположим, что $\operatorname{gap}(g_k) < \infty$. Так как $\operatorname{gap}(g_0) = \infty$ и $\operatorname{gap}(g_k) < \infty$, мы можем найти такое p, что

$$\operatorname{gap}(g_k) = \operatorname{gap}(g_{k-1}) = \ldots = \operatorname{gap}(g_p) < \operatorname{gap}(g_{p-1}).$$

Аналогично предыдущему случаю $g_k^{a_k} = g_{p-1}^{a_{p-1}\ldots a_k} - R$, где R можно представить суммой k-стандартных мономов и $g_{k+1} = g_{p-1}^{a_{p-1}\ldots a_k} - R - r_k$. Поскольку

$$\operatorname{gap}(g_{p-1}^{a_{p-1}\ldots a_k}) = \operatorname{gap}(g_{p-1}) > \operatorname{gap}(g_k) = \operatorname{gap}(g_{p-1}^{a_{p-1}\ldots a_k} - R) = \operatorname{gap}(g_p),$$

мы можем заключить, что наибольшим отрицательным k-стандартным мономом в представлении R суммой k-стандартных мономов является $\nu_{p-1}g_p^{a_p-1}\ldots g_k^{a_k-1}$, где ν_{p-1} — наибольший отрицательный $(p-1)$-стандартный моном в r_{p-1}. Следовательно,

$$\deg_z(\nu_{p-1}g_p^{a_p-1}\ldots g_{k-1}^{a_k-1}) = \\ = \deg_z(\nu_{p-1}) + (a_p - 1)m_p + \ldots + (a_k - 1)m_k > a_k m_k,$$

потому что $\deg_z(\nu_{p-1}) > m_p$ и $a_j m_j > m_{j+1}$ при любом j. Но $\deg_z(r_k) < a_k m_k$, и рассматриваемый моном не может быть слагаемым в r_k. Как и в предыдущем случае, наибольшие отрицательные мономы r_k и $g_k^{a_k}$ различны. Лемма доказана. □

Замечание для читателя, знакомого с полями конечной характеристики

В процессе работы алгоритма отрицательные степени f действительно появляются, если характеристика конечна и делит m и n. (Проверьте пример перед формальным описанием алгоритма для характеристики, равной двум.) Наше доказательство не работает в этом случае, поскольку функция gap перестаёт удовлетворять условию (б).

Итак, мы доказали, что все g_i являются многочленами от f и g, а значит, и все стандартные мономы $g_0^{j_0} \dots g_s^{j_s}$ тоже многочлены от f и g. Мы заметили при доказательстве леммы 2, что любой многочлен Q от f и g, у которого $\deg_g(Q) < a_s \deg_g(g_s)$, является суммой положительных и отрицательных s-стандартных мономов. Теперь мы можем заметить, что отрицательных s-стандартных мономов в этой сумме нет. Действительно, если $Q = q_0(f)g^l + \dots + q_l$, где $q_i \in \mathbb{Q}[f]$, то найдём s-стандартный моном $\mathbf{m}$ степени l по g, у которого $\mathrm{pow}_f(\mathbf{m}) = 0$. Тогда $Q - q_0\mathbf{m}$ — многочлен, степень которого меньше l, и мы можем применить индукцию по степени.

Для любого многочлена $H(x, y)$ от двух переменных найдётся многочлен $Q(x, y)$, для которого $\deg_y(Q(x, y)) < a_s \deg_g(g_s)$ и $Q(f(z), g(z)) = H(f(z), g(z))$. Достаточно поделить $H(x, y)$ на $P(x, y)$ с остатком, рассматривая их как многочлены от y с коэффициентами — многочленами от x. Тогда $H(x, y) = a(x, y)P(x, y) + Q(x, y)$.

Таким образом, любой многочлен $H(f(z), g(z))$ может быть записан двумя способами: с помощью обычных мономов,

$$H(f(z), g(z)) = \sum_{i,j} h_{i,j} f(z)^i g(z)^j,$$

и с помощью положительных s-стандартных мономов. Более того, если s-стандартные мономы найдены, то можно сказать, какой многочлен $h(z)$ от одной переменной может быть записан как многочлен от $f(z)$ и $g(z)$. По лемме 1(а), степени по z у всех s-стандартных мономов различны. Поэтому, чтобы узнать, является ли $h(z)$ многочленом от $f(z)$ и $g(z)$, нужно проверить, существует ли s-стандартный моном степени $\deg_z(h)$. Если нет, то $h \notin \mathbb{Q}[f(z), g(z)]$, где $\mathbb{Q}[f(z), g(z)]$ — множество всех многочленов от $f(z)$ и $g(z)$. Если же такой s-стандартный моном $\mathbf{m}_1$ нашёлся, то нужно заменить $h(z)$ на $h_1(z) = h(z) - q_1\mathbf{m}_1$, где рациональное число q_1 выбрано так, что $\deg_z(h(z) - q_1\mathbf{m}_1) < \deg_z(h(z)$. Понятно, что h_1 — многочлен от $f(z)$ и $g(z)$ тогда и только тогда, когда h — многочлен от $f(z)$ и $g(z)$. Повторяя проверку для h_1, мы либо узнаем, что h и h_1 не многочлены от $f(z)$ и $g(z)$, либо получим многочлен h_2, причём $\deg_z(h_2) < \deg_z(h_1)$.

Таким образом, не больше чем за $\deg_z(h)$ шагов мы узнаем, является ли h многочленом от $f(z)$ и $g(z)$, и, если является, найдём такой многочлен H от двух переменных, что $h(z) = H(f(z), g(z))$.

Если f и g удовлетворяют условиям теоремы AMC, то $\mathbb{Q}[f(z), g(z)] = \mathbb{Q}[z]$. Следовательно, любой многочлен от z является суммой положительных s-стандартных мономов и для произвольного натурального числа d существует положительный s-стандартный моном, имеющий степень d по z. Существует такой моном и для d_0. Поскольку d_0 делится на себя, по лемме 1(a) этот моном равен $f^i g_0^j$, где $in + jm = d_0$ и $0 \leqslant j < a_0$, а поскольку он положительный, $i \geqslant 0$. Так как d_0 — это наибольший общий делитель n и m, такое равенство возможно, только если $n = d_0$ или $m = d_0$.

Список литературы

[1] *Segre B.* Corrispondenze di Möbius e trasformazioni cremoniane intere // Atti Accademia Sci. Torino. 1956–1957. V. 91. P. 3–19.

[2] *Canals I., Lluis E.* Acerca de un resultado de Segre // Anales del Instituto de Matemáticas. Universidad Nacional Autónoma de México. 1970. V. 10. P. 1–15.

[3] *Abhyankar S. S., Moh T. T.* Embeddings of the line in the plane // J. Reine Angew. Math. 1975. V. 276. P. 148–166.

[4] *Abhyankar S. S., Moh T. T.* Newton — Puiseux expansion and generalized Tschirnhausen transformation. I, II // J. Reine Angew. Math. 1973. V. 260. P. 47–83; 1973. V. 261, P. 29–54.

[5] *Suzuki M.* Propriétés topologiques des polynômes de deux variables complexes, et automorphismes algébriques de l'espace $\mathbb{C}^2$ // J. Math. Soc. Japan. 1974. V. 26. P. 241–257.

Леонид Григорьевич Макар-Лиманов, Университет Уэйна,
Мичиган, США

lml@wayne.edu