Алгоритм вычисления минимального строго λ-низкого числа, кратного данному

Денис Крыськов[1]

Abstract

Сформулирован алгоритм, который для произвольного натурального x находит минимальное y со свойствами

- y — лямбда-низкое число;
- для любого простого p, делящего y, число $p-1$ также делит y;
- x делит y.

Метод нахождения такого числа ранее был неизвестен; Ю.В.Нестеренко [Nest] сформулировал алгоритм нахождения **неминимального** числа с такими свойствами.

Ключевые слова: лямбда-низкое число, строго лямбда-низкое число, дискретный логарифм.

Через $\mathcal{P}$ обозначим множество всех нечётных простых чисел.

Основным результатом настоящей статьи является алгоритм нахождения для натурального числа x минимального натурального y, обладающего тремя свойствами

$$\begin{array}{l} y \text{ — } \lambda\text{-низкое;} \\ \forall p \in \mathcal{P}\ (p \mid y \Longrightarrow (p-1) \mid y); \end{array} \tag{1}$$

$$x \mid y \tag{2}$$

Этот результат улучшает один из результатов статьи [Nest], а именно алгоритм нахождения не очень большого числа, обладающего свойствами (1)–(2). Насколько известно автору, никаких алгоритмов нахождения минимального числа со свойствами (1)–(2) ранее не было известно.

Порядок изложения следующий. В разделе 1 мы знакомим читателя с λ-низкими и строго λ-низкими числами. В разделе 2 мы формулируем обещанный алгоритм; в разделе 3 доказываем его корректность. Заодно мы обнаруживаем некоторые свойства λ-низких чисел. К примеру, множество строго λ-низких чисел оказывается замкнуто относительно операций вычисления наибольшего общего делителя $\gcd(\square, \square)$ и наименьшего общего кратного $\mathrm{lcm}(\square, \square)$.

[1] http://tiny.cc/DKryskov

1 Строго λ-низкое число

Вместо $\frac{\mathbb{Z}}{m\cdot\mathbb{Z}}$ будем писать Z_m. Мы сохраняем некоторые обозначения статьи [Nest], в частности $\nu_{\square}(\square)$, $\lambda(\square)$ and $Q(\square,\square)$.

При $x, y \in \mathbb{N}$ $\nu_x(y)$ обозначает степень, в которой x входит в y:

$$\nu_x(y) := \max\left\{z \in \mathbb{N}\bigcup\{0\} : x^z \mid y\right\}.$$

$\lambda(x)$ обозначает функцию Кармайкла — экспоненту группы $(Z_x, *)$. И $Q(x, y)$ обозначает частное Ферма для x по модулю y:

$$Q(x, y) := \frac{x^{\lambda(y)} - 1}{y} \bmod y\ .$$

Ризель в работе [Ries] назвал λ-низким натуральное n, обладающее двумя свойствами $\nu_2(n) = \nu_2(\lambda(n)) + 2$; для любого $p \in \mathcal{P}$, делящего n, $\nu_p(n) = \nu_p(\lambda(n)) + 1$.

Назовём число $y \in \mathbb{N}$ строго λ-низким, если оно обладает двумя свойствами (1).

Нестеренко [Nest] доказал, что в некоторых случаях дискретный логарифм по модулю таких чисел легко вычислить. Мы переформулируем соответствующий результат в виде теоремы 1.

Теорема 1 *Пусть r, m — натуральные числа, r — строго λ-низкое. Пусть разложение r и m по степеням простых имеет вид*

$$\begin{aligned} r &= 2^{k_0} \cdot p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_t^{k_t} \quad , \\ m &= 2^{k_0+2} \cdot p_1^{k_1+1} \cdot p_2^{k_2+2} \cdot \ldots \cdot p_t^{k_t+1} \quad . \end{aligned}$$

Пусть также $\gamma, \gamma_0, \gamma_1, \ldots \gamma_t$ — натуральные числа со свойствами

$$\begin{aligned} &\forall i \in \overline{1,t} \quad \gamma \equiv \gamma_i \pmod{p_i^{2\cdot k_i}}, \quad \gamma \equiv \gamma_0 \pmod{2^{2\cdot k_0}}, \\ &\nu_2(\gamma_0^2 - 1) = 3, \end{aligned}$$

число γ_i максимального порядка по модулю $p_i^{2\cdot k_i}$ при $i \in \overline{1,t}$.

Пусть g — класс вычетов по модулю m, содержащий число γ. Пусть G — подгруппа $(Z_m, *)$, образованная g.

Тогда отображение $x \longmapsto Q(x, r)$ из $(G, *)$ в $(Z_r, +)$ является изоморфизмом.

Из условий теоремы 1 следует, что m также строго λ-низкое (мы докажем это ниже).

Таким образом, если m и $r = \lambda(m)$ строго λ-низкие, и их разложение на простые множители различается только в степенях, тогда в группе $(Z_m, *)$ существует циклическая подгруппа максимального порядка G такая, что для нахождения дискретного логарифма в группе G достаточно вычислить частное Ферма по модулю r и затем решить сравнение по модулю r.

Возьмём для примера $m = 2^6 \cdot 3^3 \cdot 13^3 \cdot 53^2$, $r = 2^4 \cdot 3^2 \cdot 13^2 \cdot 53$. Выберем минимально возможными числа γ_i: $(3, 2, 2, 2)$, вычислим $\gamma = 682337855747$, $g = \gamma \bmod m = 10497505475$. Выберем $a = g^{99} \bmod m, \quad b = g^{23} \bmod m$. Тогда

$$\begin{array}{l} Q(g, r) = 38119, \\ a = 626675291, \quad Q(a, r) = 3^2 \cdot 5 \cdot 7 \cdot 17 \cdot 223, \\ b = 8839623371, \quad Q(b, r) = 23 \cdot 38119. \end{array}$$

Оба равенства $a^x \equiv b \pmod m$ и $Q(a, r) \cdot x \equiv Q(b, r) \pmod r$ неразрешимы относительно x, так как порядок a в группе $(G, *)$ меньше b, а $Q(a, r)$ делится на 9, в то время как $Q(b, r)$ не делится.

Напротив, соотношения $b^x \equiv a \pmod m$ и $Q(b, r) \cdot x \equiv Q(a, r) \pmod r$ являются разрешимыми и их общим решением является $x = 616869$. Для каждого из двух соотношений это решение единственное в диапазоне от 0 до $r - 1$.

Изоморфизм групп $(G, *) \cong (Z_r, +)$ обеспечивает, что для любых $u, v \in G$ два соотношения $u^x \equiv v \pmod m$ and $Q(u, r) \cdot x \equiv Q(v, r) \pmod r$ имеют одинаковое (возможно пустое) множество решений. Именно так и случилось в рассмотренном примере.

2 Вычисление минимального строго λ-низкого кратного

Нестеренко [Nest] определил функцию $R(\square) : \mathbb{N} \longrightarrow \mathbb{N}$ такую, что число $y = R(x)$ обладает свойствами (1)–(2) и

$$log_2 y < 3 \cdot (log_2 x)^2 \quad .$$

Обозначим через $\tilde{R}(x)$ минимальное y со свойствами (1)–(2). Вычисляя значения этих функций для маленьких x, обнаруживаем несовпадение:

$$\begin{array}{l} R(7) = 2016 = 4 \cdot \tilde{R}(7) \\ R(21) = 2016 = 4 \cdot \tilde{R}(21) \\ R(43) = 7281792 = 48 \cdot \tilde{R}(43) \\ R(311) = 3425143954176 = 80 \cdot \tilde{R}(311) \end{array} \quad .$$

В этом разделе мы определим функцию $\breve{R}(\square)$. В следующем разделе мы докажем, что $\breve{R}(x) = \tilde{R}(x)$ для любого $x \in \mathbb{N}$.

Для любых чисел k_i и p_i, таких, что $k_0 \in \mathbb{N} \bigcup \{0\}$; $k_i \in \mathbb{N}$, $p_i \in \mathcal{P}$, $i \in \overline{1, t}$; $p_1 < p_2 < \ldots < p_t$, положим

$$\Delta\left(2^{k_0} \cdot p_1^{k_1} \cdot p_2^{k_2} \cdot \ \ldots \cdot p_t^{k_t}\right) := p_1^{k_1+1} \cdot p_2^{k_2+1} \cdot \ \ldots \cdot p_t^{k_t+1} \ .$$

В силу единственности разложения на простые сомножители целочисленная функция $\Delta(\square)$ определена корректно.

Для $y \in \mathbb{N}$ положим

$$\tau(y) := \max\{\nu_2(q-1) : \ q \in \mathcal{P}, \ q \mid y\} \quad .$$

Определим рекурсивно функцию $S(\square, \square)$, $S : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$. Функция S вычисляется согласно 4 правилам 1-4:

1. $S(1, x) := x$, $x \in \mathbb{N}$.
2. $S(2^x \cdot y, z) := S(y, z), \quad y \in 2 \cdot \mathbb{N} + 1, \ x \in \mathbb{N}$.
3. $S(q^x, y) := S(q - 1, \operatorname{lcm}(y, \Delta(q-1) \cdot q^x)), \quad q \in \mathcal{P}$.
4. $S(p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_t^{k_t}, x) := \operatorname{lcm}\left(x, S(p_1^{k_1}, 1), S(p_2^{k_2}, 1), \ldots S(p_t^{k_t}, 1)\right), \quad t > 1, \ p_i \in \mathcal{P}, \ k_i \in \mathbb{N}, \ p_1 < p_2 < \ldots < p_t$.

Для примера посчитаем $S(3 \cdot 53^2, 1)$.

$$S(3 \cdot 53^2, 1) = \operatorname{lcm}(1, S(3,1), S(53^2, 1)) = \operatorname{lcm}(S(3,1), S(53^2, 1)) \ .$$

$$S(3,1) = S(2, \operatorname{lcm}(1, \Delta(2) \cdot 3)) = S(2,3) = S(1,3) = 3 \quad .$$

$$S(53^2, 1) = S(52, \operatorname{lcm}(1, \Delta(52) \cdot 53^2)) = S(52, 13^2 \cdot 53^2) = S(13, 13^2 \cdot 53^2) =$$
$$S(12, \operatorname{lcm}(13^2 \cdot 53^2, \Delta(12) \cdot 13)) = S(12, \operatorname{lcm}(13^2 \cdot 53^2, 3^2 \cdot 13)) = S(12, 3^2 \cdot 13^2 \cdot 53^2) =$$
$$S(3, 3^2 \cdot 13^2 \cdot 53^2) = S(2, \operatorname{lcm}(3^2 \cdot 13^2 \cdot 53^2, \Delta(2) \cdot 3)) = S(2, 3^2 \cdot 13^2 \cdot 53^2) =$$
$$S(1, 3^2 \cdot 13^2 \cdot 53^2) = 3^2 \cdot 13^2 \cdot 53^2 \quad .$$

Поэтому

$$S(3 \cdot 53^2, 1) = \operatorname{lcm}(3, 3^2 \cdot 13^2 \cdot 53^2) = 3^2 \cdot 13^2 \cdot 53^2 \ .$$

Определим теперь функцию $\breve{R}(\square)$:

$$\breve{R}(x) := S(x,1) \cdot 2^{\max(3, \nu_2(x), 2 + \tau(S(x,1)))} \ .$$

Пользуясь вычисленным ранее, найдём

$$\breve{R}(3 \cdot 53^2) = 2^4 \cdot 3^2 \cdot 13^2 \cdot 53^2 \ .$$

Довести пример до конца (то есть доказать равенство $\tilde{R}(3 \cdot 53^2) = \breve{R}(3 \cdot 53^2)$) предоставим читателю.

3 Доказательство правильности алгоритма

Наша конечная цель — доказательство равенства $\tilde{R}(x) = \breve{R}(x)$ для всех целых x. Нам потребуются большое количество вспомогательных результатов.

Теорема 2 *Пусть* $x, y \in \mathbb{N},\ \gcd(x,y) = 1$. *Тогда*

$$\lambda(x \cdot y) = \operatorname{lcm}\Big(\lambda(x), \lambda(y)\Big)\ .$$

Доказательство: Символом $\times$ обозначим прямое внешнее произведение алгебр. При доказательстве этой теоремы $e(U)$ будет обозначать экспоненту группы U.

Не вызывает сомнения, что

- кольцо $Z_{x\cdot y}$ изоморфно произведению $Z_x \times Z_y$.
- для групп A и B число $e(A \times B)$ равняется $\operatorname{lcm}\Big(e(A), e(B)\Big)$.

Эти два свойства общеизвестны; второе зафиксировано в [GP].

Тогда

$$\lambda(x \cdot y) = e(Z_{x\cdot y}) = e(Z_x \times Z_y) = \operatorname{lcm}\Big(e(Z_x), e(Z_y)\Big) = \operatorname{lcm}\Big(\lambda(x), \lambda(y)\Big)\ .$$

□

Иногда нам будет удобно писать $y \ \vdots\ x$ вместо $x \mid y$.

Теорема 3 $\alpha, \beta \in \mathbb{N},\ \alpha \mid \beta \quad \Longrightarrow \quad \lambda(\alpha) \mid \lambda(\beta)$.

Доказательство: Разложим α по степеням простых:

$$\alpha = \prod_{i\in I} a_i^{\delta_i}\ ,$$

$a_i \in \{2\} \bigcup \mathcal{P},\ \delta_i \in \mathbb{N}$.

Тогда β может быть представлена в виде

$$\beta = \prod_{i\in I} a_i^{\delta_i+\epsilon_i} \cdot \gamma\ ,$$

где $\epsilon_i \geq 0$ и $\gcd(\prod_{i\in I} a_i^{\delta_i+\epsilon_i}, \gamma) = 1$.

Будем считать, что читателю известна формула вычисления функции Кармайкла. Также предположим, что читатель докажет два тезиса

$$\begin{array}{l} c \in \{2\} \bigcup \mathcal{P}, \mu \in \mathbb{N}, \delta \in \{0\} \bigcup \mathbb{N} \Longrightarrow \lambda(c^{\mu+\delta}) \ \vdots\ \lambda(c^{\mu}) \\ x_j, y_j \in \mathbb{N} \Longrightarrow \operatorname{lcm}\Big(\{x_j \cdot y_j : j \in J\}\Big) \ \vdots\ \operatorname{lcm}\Big(\{x_j : j \in J\}\Big) \end{array}\ . \tag{3}$$

По теореме 2, конструктивному определению функции Кармайкла и соотношениям (3) получаем, что

$$\lambda(\beta) \ \vdots\ \lambda\left(\prod_{i\in I} a_i^{\delta_i+\epsilon_i}\right) = \operatorname{lcm}\left(\left\{\lambda(a_i^{\delta_i+\epsilon_i}) : i \in I\right\}\right) \ \vdots\ \vdots\ \operatorname{lcm}\left(\left\{\lambda(a_i^{\delta_i}) : i \in I\right\}\right) = \lambda(\alpha)\ . \tag{4}$$

Из тезиса (4) и транзитивности отношения $\vdots$ теорема следует. □

Теорема 4 *Если числа $x,\ y$ строго λ-низкие, то таково и число* $\gcd(x,y)$.

Доказательство: Положим $d := \gcd(x,y)$. По теореме 3

$$\lambda(d) \mid \lambda(x)\ . \tag{5}$$

Мы вначале докажем, что d является λ-низким.

Согласно [Nest, §2], для любых $m \in \mathbb{N},\ p \in \mathcal{P}$

$$\nu_2(m) \le \nu_2(\lambda(m)) + 2, \quad \nu_p(m) \le \nu_p(\lambda(m)) + 1\ . \tag{6}$$

Без сомнений $\nu_2(d) = \min\Big(\nu_2(x), \nu_2(y)\Big)$. Не ограничивая общности будем считать, что $\nu_2(x) \le \nu_2(y)$. Согласно определению λ-низкого числа и (5)

$$\nu_2(d) = \nu_2(x) = \nu_2(\lambda(x)) + 2 \ge \nu_2(\lambda(d)) + 2\ . \tag{7}$$

Подставляя d вместо m в равенство (6), получаем, что число $\nu_2(d)$ не меньше и не больше, чем $\nu_2(\lambda(d)) + 2$. Это означает, что

$$\nu_2(d) = \nu_2(\lambda(d)) + 2\ .$$

Аналогично доказываеся, что для произвольного нечётного простого p, делящего d, $\nu_p(d) = \nu_p(\lambda(d)) + 1$.

Поэтому число d является λ-низким.

Зафиксируем $p \in \mathcal{P}$ такое, что $p \mid d$. Из определения НОД

$$p \mid x, p \mid y \Longrightarrow (p-1) \mid x, (p-1) \mid y \Longrightarrow (p-1) \mid d\ .$$

Следовательно, $\forall p \in \mathcal{P}\ (p \mid d \Longrightarrow (p-1) \mid d)$. Все свойств строго λ-низкого числа выполняются. $\square$

Для произвольных $z, w \in \mathbb{N}$ через $z \dagger w$ обозначим $\min\left\{\frac{z}{w^x} : x \in \mathbb{N}\bigcup\{0\},\ \frac{z}{w^x} \in \mathbb{N}\right\}$.

Для $x \in \mathbb{N}$ положим $\tilde{H}(x) := \tilde{R}(x) \dagger 2$.

Теорема 5 $x,\ y \in \mathbb{N},\ x \mid y \quad \Longrightarrow \quad \tilde{H}(x) \mid \tilde{H}(y),\ \tilde{R}(x) \mid \tilde{R}(y)\ .$

Доказательство: Вначале мы докажем, что $\tilde{R}(x) \mid \tilde{R}(y)$. Обозначим эти два числа через u и v.

Предположим противное: u не делит v. Положим $z := \gcd(u,v)$. По сделанному предположению $z < u$.

$x \mid u$, $x \mid y \mid v$, следовательно $x \mid z$. По теореме (4) число z строго λ-низкое.

Итак, $x \mid z < \tilde{R}(x)$, при этом z строго λ-низкое. Это противоречит определению $\tilde{R}(\square)$.

Наше предположение привело к противоречию. Это означает, что верно обратное:

$$\tilde{R}(x) \mid \tilde{R}(y)\ . \tag{8}$$

Соотношение $\tilde{H}(x) \mid \tilde{H}(y)$ непосредственно следует из (8) и определения $\tilde{H}(\square)$. $\square$

Теорема 6 *Если число x строго λ-низкое, $r \in \{2\} \bigcup \mathcal{P}$, $r \mid x$, то $x \cdot r$ также строго λ-низкое.*

Доказательство: Обозначим $\alpha := \nu_r(x)$, $y := x \dagger r$. По теореме 2

$$\lambda(x) = \operatorname{lcm}\left(\lambda(r^\alpha), \lambda(y)\right) \ , \tag{9}$$

$$\lambda(x \cdot r) = \operatorname{lcm}\left(\lambda(r^{\alpha+1}), \lambda(y)\right) \ . \tag{10}$$

Вначале рассмотрим случай $r = 2$.

Так как x является λ-низким, $\nu_2(\lambda(x)) = \alpha - 2$. Из равенства (9)

$$\nu_2(\lambda(y)) \leq \alpha - 2 \ . \tag{11}$$

Пользуясь равенством (11), преобразуем правую часть (9) и (10) — исключим малые степени числа 2 и операцию вычисления НОК:

$$\lambda(x) = \operatorname{lcm}\left(2^{\alpha-2}, \lambda(y) \dagger 2\right) = 2^{\alpha-2} \cdot (\lambda(y) \dagger 2)$$
$$\lambda(2 \cdot x) = \operatorname{lcm}\left(2^{\alpha-1}, \lambda(y) \dagger 2\right) = 2^{\alpha-1} \cdot (\lambda(y) \dagger 2)$$

Поэтому

$$\lambda(2 \cdot x) = 2 \cdot \lambda(x) \ . \tag{12}$$

Теперь, используя равенство (12), проверим определение λ-низкого числа применительно к $2 \cdot x$. Зафиксируем p — нечётный простой делитель $2 \cdot x$.

$$\begin{array}{l} \nu_2\left(\lambda(2 \cdot x)\right) = 1 + \nu_2\left(\lambda(x)\right) = \nu_2(x) - 1 = \nu_2(2 \cdot x) - 2 \\ \nu_p\left(\lambda(2 \cdot x)\right) = \nu_p\left(\lambda(x)\right) = \nu_p\left(x\right) - 1 = \nu_p\left(2 \cdot x\right) - 1 \end{array} \ .$$

Мы только что доказали, что $x \cdot 2$ является λ-низким.

Случай $r > 2$ рассматривается по той же схеме. Вначале надо доказать, что $\lambda(r \cdot x) = r \cdot \lambda(x)$ (на основании того факта, что x является λ-низким, и равенств (9)–(10)). Затем следует в трёх случаях $p = 2$, $p = r$ и $p \in \mathcal{P} \setminus \{r\}$ проверить разность $\nu_p(x \cdot r) - \nu_p\left(\lambda(x \cdot r)\right)$, которая должна равняться 2,1,1. Таким образом будет доказано, что число $x \cdot r$ является λ-низким. Мы пропускаем эту часть доказательства и предоставляем читателю возможность воспроизвести её самостоятельно.

Проверим теперь последнее свойство строго λ-низкого числа. Зафиксируем одно из простых чисел, делящих $r \cdot x$, обозначим его p. Тогда p делит x, слкедовательно $p - 1$ делит x, следовательно, $p - 1$ делит $r \cdot x$.

Все свойства строго λ-низкого числа выполняются. □

Теорема 7 *Пусть x строго λ-низкое; $x \mid y$; два множества $\{z \in \mathcal{P} : z \mid x\}$ и $\{z \in \mathcal{P} : z \mid y\}$ совпадают. Тогда число y также является строго λ-низким.*

Доказательство: Достаточно многократно применить теорему 6. □

Теорема 8 *Пусть число x строго λ-низкое, $p \in \mathcal{P}$, $p \mid \lambda(x)$. Тогда $p \mid x$.*

Доказательство: Предположим, что, наоборот, p не делит x.

Разложим x по степеням простых:

$$x = 2^{\alpha_0} \cdot q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdot \dots \ .$$

Согласно конструктивному определению функции Кармайкла

$$p \mid \operatorname{lcm}\left(2^{\alpha_0-2}, q_1^{\alpha_1-1} \cdot (q_1-1), q_2^{\alpha_2-1} \cdot (q_2-1), \dots\right) \ .$$

Удалим из правой части числа, не делящиеся на p:

$$p \mid \operatorname{lcm}(q_1-1, q_2-1, \dots) \ .$$

Тогда для некоторого i $p|(q_i-1)$, причём $q_i \in \mathcal{P}, q_i \mid x$. Так как x строго λ-низкое, $q_i - 1$ делит x, так что $p \mid x$.

Таким образом, при предположении "p не делит x", мы доказали утверждение "p делит x". Полученное противоречие показывает, что гипотеза неверна. Теорема доказана.□

Теорема 9 *Если $v \in \mathbb{N},\ u = \tilde{H}(v),\ p \in \mathcal{P},\ p \mid \lambda(u)$, то $p \mid u$.*

Доказательство: Достаточно проименить теорему 8 к $x := \tilde{R}(v)$; учесть, что $\lambda(x)$ может отличаться от $\lambda(u)$ только в степенях числа 2.□

Мы определили операцию $\dagger$ на целых числах. Переопределим операцию на случай, когда правый операнд — множество чисел:

$$\alpha \dagger \{\beta_0, \beta_1, \ \dots\} := \alpha \dagger \beta_0 \dagger \beta_1 \dagger \dots \ .$$

Если B — пустое множество, то по определению $\alpha \dagger B := \alpha$.

Теорема 10 *Если числа x, y строго λ-низкие, то таково же и число* $\operatorname{lcm}(x, y)$.

Доказательство: Положим $z := \operatorname{lcm}(x, y)$, $R := \{2\} \bigcup \{u \in \mathcal{P} : u \mid \gcd(x, y)\}$, $S := \{u \in \mathcal{P} : u \mid x\} \setminus R$, $T := \{u \in \mathcal{P} : u \mid y\} \setminus R$. Зададим 5 натуральных чисел v, s, t, α, β равенствами

$$\begin{array}{l} v := \operatorname{lcm}(x \dagger S, y \dagger T) \\ s := x \dagger R,\ \alpha := v \cdot s \\ t := y \dagger R,\ \beta := v \cdot t \end{array} \ .$$

Заметим, что для любого простого p выполняются два равенства

$$\nu_p(\alpha) = \begin{cases} \nu_p(x),\ p \in S, \\ \max\left(\nu_p(x), \nu_p(y)\right), p \in R \\ 0,\ \text{иначе} \end{cases} ,$$

$$\nu_p(\beta) = \begin{cases} \nu_p(x),\ p \in T, \\ \max\left(\nu_p(x), \nu_p(y)\right), p \in R \\ 0,\ \text{иначе} \end{cases} .$$

Кроме того, числа v, s, t попарно взаимно-просты;

$$z = v \cdot s \cdot t \ . \tag{13}$$

Применяя теорему 7 к x и α, получаем, что α является строго λ-низким. Аналогично число β строго λ-низкое.

По теоерме 2 верны 3 равенства

$$\begin{array}{l} \lambda(z) = \mathrm{lcm}\left(\lambda(v), \lambda(s), \lambda(t)\right) \\ \lambda(\alpha) = \mathrm{lcm}\left(\lambda(v), \lambda(s)\right) \\ \lambda(\beta) = \mathrm{lcm}\left(\lambda(v), \lambda(t)\right) \end{array} \ .$$

Отсюда

$$\lambda(z) = \mathrm{lcm}\left(\lambda(\alpha), \lambda(\beta)\right) \ . \tag{14}$$

Используя равенство (14) и тот факт, что числа α, β являются строго λ-низкими, легко доказать искомое.

Предположим, что $p \in \mathcal{P},\ p \mid z$. Тогда p принадлежит одному из трёх множеств R, S, T, и выполняется равенство

$$\nu_p(\lambda(z)) = \max\{\nu_p(\lambda(\alpha)), \nu_p(\lambda(\beta))\} \ .$$

Если $p \in R$, то

$$\nu_p(\lambda(z)) = \max\{\nu_p(\alpha) - 1, \nu_p(\beta) - 1\} = \nu_p(v) - 1 = \nu_p(z) - 1 \ .$$

В случае $p \in S$ имеет место равенство $\nu_p(\beta) = 0$, отсюда по теореме 8 $\nu_p(\lambda(\beta)) = 0$, так что

$$\nu_p(\lambda(z)) = \nu_p(\lambda(\alpha)) = \nu_p(\alpha) - 1 = \nu_p(z) - 1 \ .$$

По соображениям симметрии случай $p \in T$ можно не рассматривать.

Мы проверили, что для любого $p \in \mathcal{P}$, делящего z, $\nu_p(\lambda(z)) = \nu_p(z) - 1$.

А поскольку

$$\nu_2(\lambda(z)) = \max\{\nu_2(\alpha) - 2, \nu_2(\beta) - 2\} = \nu_p(v) - 2 = \nu_p(z) - 2 \ ,$$

z является λ-низким.

Вновь используя (13), проверим утверждение $p \in \mathcal{P},\ p \mid z \Longrightarrow (p-1) \mid z$.

$$p \in \mathcal{P},\ p \mid z \Longrightarrow p \mid \alpha \text{ or } p \mid \beta \Longrightarrow (p-1) \mid \alpha \text{ or } (p-1) \mid \beta \Longrightarrow (p-1) \mid z \ .$$

Итак, z действительно строго λ-низкое.$\square$

Теорема 11 *Если* $\alpha, \beta \in \mathbb{N},\ \gcd(\alpha, \beta) = 1$, *то*

$$\begin{array}{l} \tilde{H}(\alpha \cdot \beta) = \mathrm{lcm}\left(\tilde{H}(\alpha), \tilde{H}(\beta)\right) \\ \tilde{R}(\alpha \cdot \beta) = \mathrm{lcm}\left(\tilde{R}(\alpha), \tilde{R}(\beta)\right) \end{array} \ .$$

Доказательство: Равенство $\tilde{H}(\square)$ следует из равенства для $\tilde{R}(\square)$, поэтому достаточно доказать последнее.

Положим $x := \tilde{R}(\alpha \cdot \beta)$, $y := \operatorname{lcm}\left(\tilde{R}(\alpha), \tilde{R}(\beta)\right)$. По теореме 5

$$\tilde{R}(\alpha) \mid x, \quad \tilde{R}(\beta) \mid x \ . \tag{15}$$

Следовательно, $y \mid x$. Поэтому выполняется либо равенство $y = x$, которое нам надо доказать, либо неравенство

$$y < x \ . \tag{16}$$

Предположим, что теорема неверна, и выполняется неравенство (16).

Согласно (15) каждое из чисел α, β делит x. Ясно также, что эта пара чисел делит y. Обозначим $z := \gcd(x, y)$. Из соотношений $(\alpha \cdot \beta) \mid x$, $(\alpha \cdot \beta) \mid y$ следует, что $(\alpha \cdot \beta) \mid z$.

По теореме 10 число y строго λ-низкое. Следовательно, по теореме 4 z также строго λ-низкое. А по предположению (16) $z < x$.

Существование такого числа z противоречит минимальности x — ведь x должен быть минимальным строго λ-низким, делящимся на $\alpha \cdot \beta$. Получено противоречие, предположение неверно. □

Теорема 12 *Для любого* $y \in \mathbb{N}$

$$\tilde{H}(y \dagger 2) = \tilde{H}(y) \ .$$

Доказательство: Положим $\alpha := \nu_2(y)$, $x := y \dagger 2$. По теореме 11

$$\tilde{H}\left(2^{\alpha} \cdot x\right) = \operatorname{lcm}\left(\tilde{H}(2^{\alpha}), \tilde{H}(x)\right) = \tilde{H}(x).$$

□

Теорема 13 *Пусть* $x \in 2 \cdot \mathbb{N} + 1$*;* $\mathcal{H}$ *— область значений фунцкии* $\tilde{H}(\square)$*:*

$$\mathcal{H} := \tilde{H}(\mathbb{N}) \ . \tag{17}$$

Тогда $\tilde{H}(x) = \min\{u \in \mathcal{H} : x \mid u\}$.

Доказательство: Зафиксируем $X := \{u \in \mathcal{H} : x \mid u\}$, $y := \tilde{R}(x)$, $z := \tilde{H}(x)$. Ясно, что $z \in X$. Поэтому $z \geq \min X$. Нам требуется доказать, что $z = \min X$. Предположим, что это неверно, то есть что $z > \min X$.

В этом случае существуют натуральные u, w такие, что

$$\begin{array}{l} x \mid u < z \\ u = \tilde{H}(w) \end{array} .$$

Положим $t := \tilde{R}(w)$, $s := \gcd(t, y)$.

$$s \dagger 2 = \gcd(u, y \dagger 2) \leq u < z = y \dagger 2 \ ,$$

так что $s \neq y$, а следовательно $s < y$. А так как x делит y и t, x также делит s. По теореме 4 число s строго λ-низкое.

Существование такого числа s противоречит выбору y. Значит, сделанное предположение неверно.□

Теорема 14 *Для любого* $x \in \mathbb{N}$

$$\tilde{H}\left(\tilde{H}(x)\right) = \tilde{H}(x) \ .$$

Доказательство: Положим $y := \tilde{H}(x)$, также сохраним обозначение (17).

Поскольку y нечётно, $y \mid \tilde{H}(y)$, отсюда

$$y \leq \tilde{H}(y)$$

.

По определению $\mathcal{H}$, $y \in \mathcal{H}$. Следовательно, $y \in \{u \in \mathcal{H} : y \mid u\}$. Поэтому

$$y \geq \min\{u \in \mathcal{H} : y \mid u\} \ . \tag{18}$$

По теореме 13 $\tilde{H}(y)$ равняется правой части (18). Следовательно,

$$y \geq \tilde{H}(y) \ .$$

Мы доказали, что одновременно $\tilde{H}(y) \geq y$ и $\tilde{H}(y) \leq y$.□

Теорема 15 *Пусть* $x \in \mathbb{N}$, $\tilde{H}(x) > 1$. *Тогда*

$$\max\{y \in \mathcal{P} : y \mid x\} = \max\left\{y \in \mathcal{P} : y \mid \tilde{H}(x)\right\} = \max\left\{y \in \mathcal{P} : y \mid \tilde{R}(x)\right\} \ .$$

Доказательство: Равенство $\max\left\{y \in \mathcal{P} : y \mid \tilde{H}(x)\right\} = \max\left\{y \in \mathcal{P} : y \mid \tilde{R}(x)\right\}$ очевидно. Поэтому нам требуется только доказать, что

$$\max\{y \in \mathcal{P} : y \mid x\} = \max\left\{y \in \mathcal{P} : y \mid \tilde{R}(x)\right\} \ . \tag{19}$$

Это равенство можно доказать на основании результатов [Nest] (а именно свойств функции $R(\square)$). Не претендуя на авторство равенства (19), мы проведём независимое доказательство.

Положим $z := \tilde{R}(x)$, m — левая часть (19). Предположим, что равенство не верно, то есть что правая часть больше. Тогда множество $Y := \{y \in \mathcal{P} : y > m, y \mid z\}$ непусто.

Зафиксируем $u := z \dagger Y$. В рамках сделанного предположения $x \mid u < z$. По теореме 3 $\lambda(u) \mid \lambda(z)$.

Докажем теперь, что u является строго λ-низким. Предположим, что $p \in \mathcal{P},\ p \mid u$.

$$\nu_p(\lambda(u)) \leq \nu_p(\lambda(z)) = \nu_p(z) - 1 = \nu_p(u) - 1 \ .$$

Используя неравенство (6), получаем равенство $\nu_p(\lambda(u)) = \nu_p(u) - 1$. Аналогичным способом доказывается, что $\nu_2(\lambda(u)) = \nu_2(u) - 2$. Итак, u является λ-низким.

Теперь проверим утверждение $p \in \mathcal{P},\ p \mid u \Longrightarrow (p-1) \mid u$. Зафиксируем нечётное простое p, делящее u.

$$p \mid u \Longrightarrow p \leq m, p \mid z \Longrightarrow p - 1 < m, (p-1) \mid z \Longrightarrow (p-1) \mid u \ .$$

Мы нашли число u, которое строго λ-низкое, делится на x и меньше чем z — противоречие. Значит, сделанное предположение неверно и равенство (19) выполняется. □

Теорема 16 $x \in \mathcal{P},\ k \in \mathbb{N} \quad \Longrightarrow \quad \tilde{H}(x^k) = x^k \cdot \tilde{H}\left(\Delta(x-1)\right)$.

Доказательство: Зафиксируем $s := \tilde{H}\left(\Delta(x-1)\right)$, $z := x^k \cdot s$, $y := \tilde{H}(x^k)$, $\mu := \nu_2(\tilde{R}(x^k))$.

Разложим $(x-1) \dagger 2$ по степеням простых

$$(x-1) \dagger 2 = \prod_{i \in I} p_i^{u_i} \ . \tag{20}$$

По теореме 3 $\lambda(x^k) \mid \lambda(y)$, следовательно $\prod_{i \in I} p_i^{u_i} \mid \lambda(y)$. Отсюда по теореме 9 $\prod_{i \in I} p_i \mid y$. Поскольку $2^\mu \cdot y$ λ-низкое, $\prod_{i \in I} p_i^{u_i+1} \mid y$. Согласно определению функции $\Delta(\square)$ можно переписать это соотношение в виде

$$\Delta(x-1) \mid y \ .$$

По теореме 5 получаем

$$s \mid \tilde{H}(y) \ .$$

Используя теорему 14, упростим правую часть:

$$s \mid y \ .$$

По теореме 15 x взаимно-просто с s, но x^k делит y, так что $x^k \cdot s \mid y$, или короче

$$z \mid y \ . \tag{21}$$

Зафиксируем $\beta := \nu_2(\lambda(z))$, $\gamma := \nu_2(x-1)$, $r := \tilde{R}(\Delta(x-1))$, $\alpha := 3 + \gamma + \beta + \nu_2(r)$, $w := z \cdot 2^\alpha$.

По теореме 2

$$\lambda(z) = \operatorname{lcm}\left(x^{k-1} \cdot (x-1), \lambda(s)\right) \ .$$

Так как простое x не делит $(x-1)$ или $\lambda(s)$, x^{k-1} можно вынести наружу:

$$\lambda(z) = x^{k-1} \cdot \operatorname{lcm}\left(x-1, \lambda(s)\right) \ . \tag{22}$$

Выберем произвольное $i \in I$.

$$p_i^{u_i+1} \mid \Delta(x-1) \mid s \Longrightarrow p_i^{u_i} \mid \lambda(s) \ .$$

Следовательно, $\left((x-1) \dagger 2\right) \mid \lambda(s)$. Поэтому равенство (22) можно ещё упростить:

$$\lambda(z) = x^{k-1} \cdot (\lambda(s) \dagger 2) \cdot 2^\beta \ .$$

Тогда

$$\lambda(w) = \operatorname{lcm}\left(2^{\alpha-2}, \lambda(z)\right) = x^{k-1} \cdot (\lambda(s) \dagger 2) \cdot 2^{\alpha-2} \ . \tag{23}$$

Используя равенство (23), докажем, что w строго λ-низкое.

Предположим, что $q \in \mathcal{P}$, $q \mid w$. Если $q = x$, то $\nu_q(\lambda(w)) = k-1 = \nu_q(w)-1$. В противном случае $q \mid s$, так что $\nu_q(\lambda(w)) = \nu_q(\lambda(s)) = \nu_q(s) - 1 = \nu_q(w) - 1$.

Кроме того, $\nu_2(\lambda(w)) = \alpha - 2 = \nu_2(w) - 2$. Следовательно, w является λ-низким.

Теперь выберем произвольное $q \in \mathcal{P}$, $q \mid w$; мы хотим доказать, что $(q-1) \mid w$. В случае $q = x$ имеют место соотношения

$$\begin{array}{l} x - 1 = \Big((x-1) \dagger 2\Big) \cdot 2^\gamma \\ \Big((x-1) \dagger 2\Big) \mid \Delta(x-1) \mid s \mid w \ , \\ 2^\gamma \mid 2^\alpha \mid w \end{array}$$

откуда следует, что $(x-1) \mid w$. В противном случае $q \in \mathcal{P} \setminus \{x\}$, так что $q \mid s$. $q \mid r$, r является строго λ-низким, следовательно $(q-1) \mid r \mid 2^\alpha \cdot s \mid w$.

Итак, w строго λ-низкое, поэтому

$$z \in \mathcal{H} \ , \tag{24}$$

где $\mathcal{H}$ — множество (17).

Обозначим $W := \big\{u \in \mathbb{N} : u \in \mathcal{H},\ x^k \mid u\big\}$. Согласно (24) z принадлежит W. По теореме 13 $y = \min W$, следовательно $y \le z$. В то же время согласно (21) $z \le y$. Поэтому $z = y$.$\square$

Теорема 17 *Пусть $p \in \mathcal{P},\ k \in \mathbb{N}$. Тогда*

$$\tilde{H}(p^k) = p^k \cdot \operatorname{lcm}\Big(\tilde{H}(p-1), \Delta(p-1)\Big) \ .$$

Доказательство: Положим $s := \Delta(p-1)$, $y := \operatorname{lcm}\Big(\tilde{H}(p-1), s\Big)$, $z := \tilde{H}\,(s)$. С учётом теоремы 16 достаточно доказать, что $y = z$.

По теореме 5 $\tilde{H}\,\Big((p-1) \dagger 2\Big) \mid z$. По теореме 12 $\tilde{H}\,\Big((p-1) \dagger 2\Big) = \tilde{H}(p-1)$. Следовательно,

$$\tilde{H}(p-1) \mid z \ .$$

По теореме 13 $s \mid z$. Поэтому НОК этих двух чисел делит z:

$$y \mid z \ .$$

Зафиксируем произвольное $\alpha \in \mathbb{N}$ такое, что число $2^\alpha \cdot \tilde{H}(p-1)$ строго λ-низкое. Обозначим это произведение q.

Все простые делители s также делят $p-1$, а следовательно q. Это означает, что множество простых делителей чисел q and $2^\alpha \cdot y$ совпадает; кроме того $q \mid (2^\alpha \cdot y)$. Отсюда по теореме 7 число $2^\alpha \cdot y$ является строго λ-низким. В обозначениях теоремы 13 $y \in \mathcal{H}$, поэтому

$$y \in \{u \in \mathcal{H} : s \mid u\} \ .$$

По теореме 13

$$z = \min\{u \in \mathcal{H} : s \mid u\} \ .$$

Следовательно, $y \ge z$.

Мы доказали, что $y \le z$ и $y \ge z$. Итак, $y = z$.$\square$

Теорема 18 *Пусть* $x \in \mathbb{N}, \alpha = \max\left(3, \nu_2(x), 2 + \tau\left(\tilde{H}(x)\right)\right)$. *Тогда*

$$\tilde{R}(x) = 2^\alpha \cdot \tilde{H}(x) \ .$$

Доказательство: Положим $y := \tilde{R}(x)$, $z := \lambda(y)$, $\beta := \nu_2(y)$, $s := \tilde{H}(x)$, $r := \arg\max\{\nu_2(q-1) : q \in \mathcal{P}, q \mid y\}$.

Так как y является λ-низким, $\beta \geq 3$.

Из соотношения $x \mid y$ следует, что

$$\beta \geq \nu_2(x) \ .$$

Применяя теорему 3 к соотношению $r \mid y$ получаем, что $(r-1) \mid z$. Следовательно, $\nu_2(z) \geq \nu_2(r-1) = \tau(y)$. Поскольку y является λ-низким,

$$\beta \geq 2 + \tau(y) = 2 + \tau(s) \ .$$

Итак, β не меньше любого из 3 чисел 3, $\nu_2(x)$, $2 + \tau(s)$, откуда

$$\beta \geq \alpha \ .$$

Следовательно,

$$y \geq 2^\alpha \cdot s \ . \tag{25}$$

Символом t обозначим правую часть соотношения (25). Исходя из того, что $y = 2^\beta \cdot s$ является строго λ-низким числом, докажем, что таково и t.

По теореме 2 верны два равенства $\lambda(y) = \operatorname{lcm}\left(\lambda(2^\beta), \lambda(s)\right)$, $\lambda(t) = \operatorname{lcm}\left(\lambda(2^\alpha), \lambda(s)\right)$. Избавляясь от степеней числа 2, получаем равенство

$$\lambda(y) \dagger 2 = \lambda(z) \dagger 2 \ . \tag{26}$$

Проверим определение λ-низкого числа применительно к t.

Выберем $p \in \mathcal{P}$, делящее t. Используя равенства $y \dagger 2 = z \dagger 2$ и (26), получаем

$$p \mid t \Longrightarrow p \mid y \Longrightarrow \nu_p(\lambda(y)) = \nu_p(y) - 1 \Longrightarrow \nu_p(\lambda(t)) = \nu_p(t) - 1 \ .$$

По теореме 2 и конструктивному определению функции Кармайкла

$$\nu_2(\lambda(t)) = \max(\alpha - 2, \tau(s)) = \alpha - 2 = \nu_2(t) - 2 \ .$$

Мы доказали, что t является λ-низким.

Вновь зафиксируем $p \in \mathcal{P}$, делящее t.

$$\begin{array}{l} p \mid y \Longrightarrow (p-1) \mid y \Longrightarrow ((p-1) \dagger 2) \mid t \\ \nu_2(p-1) \leq \tau(t) = \tau(s) \leq \alpha - 2 < \nu_2(t) \end{array} \ . \tag{27}$$

Из двух соотношений (27) следует, что $(p-1) \mid t$.

Таким образом, t строго λ-низкое, делится на x, не превосходит $\tilde{R}(x)$. Поэтому $t = \tilde{R}(x)$. $\square$

Теорема 19 *Пусть $u, v \in \mathbb{N}$. Тогда*

$$S(u, v) = \operatorname{lcm}\left(v, \tilde{H}(u)\right) \tag{28}$$

Доказательство: Докажем теорему индукцией по u.

При $u = 1$ равенство (28) верно, так как $\tilde{H}(1) = 1$.

Предположим, что равенство (28) выполняется при $u \in \overline{1, m}$, для некоторого $m \in \mathbb{N}$. Нам требуется доказать его при $u = m + 1$.

Предположим для начала, что u чётно: $u = 2^x \cdot y$, $y \in 2 \cdot \mathbb{N} + 1$. Тогда по правилу 2 вычисления функции $S(\square, \square)$, предположению индукции и теореме 12

$$S(u, v) = S(y, v) = \operatorname{lcm}\left(v, \tilde{H}(y)\right) = \operatorname{lcm}\left(v, \tilde{H}(2^x \cdot y)\right) \ .$$

Итак, при чётном u равенство (28) выполняется.

Рассмотрим случай нечётного u.

Предположим вначале, что u является степенью простого q. По правилу 3 вычисления $S(\square, \square)$ и предположению индукции

$$S(q^x, v) = S\left(q - 1, \operatorname{lcm}(v, \Delta(q-1) \cdot q^x)\right) = \\ \operatorname{lcm}\left(\operatorname{lcm}(v, \Delta(q-1) \cdot q^x), \tilde{H}(q-1)\right)$$

Так как числа $\Delta(q-1)$ и q^x не имеют общих делителей, мы можем преобразовать формулу:

$$S(q^x, v) = \operatorname{lcm}\left(v, q^x, \Delta(q-1), \tilde{H}(q-1)\right) = \operatorname{lcm}\left(v, q^x, \operatorname{lcm}(\Delta(q-1), \tilde{H}(q-1))\right)$$

По теореме 15 число $\operatorname{lcm}(\Delta(q-1), \tilde{H}(q-1))$ не делится на q, так что мы можем применить теорему 17:

$$S(q^x, v) = \operatorname{lcm}\left(v, q^x \cdot \operatorname{lcm}(\Delta(q-1), \tilde{H}(q-1))\right) = \operatorname{lcm}\left(v, \tilde{H}(q^x)\right) \ .$$

Итак, при $u = q^x,\ q \in \mathcal{P}$ предположение индукции выполняется.

Наконец, рассмотрим случай $u = \prod_{i=1}^{t} p_i^{k_i}$, $t > 1$, $p_1, p_2 \ldots p_t \in \mathcal{P}$, $p_1 < p_2 < \ldots < p_t$.

По правилу 4 рекурсивного определения и предположению индукции

$$S\left(\prod_{i=1}^{t} p_i^{k_i}, v\right) = \operatorname{lcm}\left(v, \tilde{H}(p_1^{k_1}), \tilde{H}(p_2^{k_2}), \ldots \tilde{H}(p_t^{k_t})\right) = \\ \operatorname{lcm}\left(v, \operatorname{lcm}(\tilde{H}(p_1^{k_1}), \tilde{H}(p_2^{k_2}), \ldots)\right) \ .$$

Применим теорему 11 и упростим формулу:

$$S(\prod_{i=1}^{t} p_i^{k_i}, v) = \operatorname{lcm}\left(v, \tilde{H}\left(\prod_{i=1}^{t} p_i^{k_i}\right)\right) \ .$$

Предположение индукции выполняется. $\square$

Теорема 20 *Для любого натурального x*

$$\breve{R}(x) = \tilde{R}(x) \ .$$

Доказательство: По теореме 19 $S(x,1) = \tilde{H}(x)$. Заменяя в определении $\breve{R}(\square)$ дважды $S(x,1)$ на $\tilde{H}(x)$, получаем формулу

$$\breve{R}(x) = 2^{\alpha} \cdot \tilde{H}(x) \ ,$$

где α именно такое, как в формулировке теоремы 18. Из теоремы 18 искомое равенство следует. □

4 Заключение

Мы улучшили один из результатов [Nest]. Число $\breve{R}(x)$ есть минимальное число, обладающее всеми полезными свойствами $R(x)$. Вычисление $\breve{R}(x)$ предположительно не сложнее вычисления $R(x)$. На самом деле, вычисление $\breve{R}(x)$ должно быть проще в связи с тем, что участвующие в вычислении числа меньше.

Это даёт основания считать, что в случае практического использования в какой-либо ситуации числа $R(x)$, можно с не меньшим успехом применить взамен число $\breve{R}(x)$.

Мы получили побочный результат: доказали, что множество строго λ-низких чисел замкнуто относительно операций $a, b \mapsto \gcd(a,b)$ и $a, b \mapsto \mathrm{lcm}(a,b)$.

Автору неизвестно о каком-либо практическом использовании числа $R(x)$ или основного результата статьи [Nest] (переформулированного в виде теоремы 1 раздела 1 настоящей статьи). Ясно, что теорема 1 указывает путь построения криптосистемы с потайным ходом, основанной на задаче дискретного логарифма в подгруппе Z_n со специально подобранным n.

Простая программа на Python, вычисляющая значения $\breve{R}(x)$ и $R(x)$ (для малых x) доступна по адресу [code]. Условия распространения: без ограничений (public domain).

References

[Ries] *Riesel H.,* Some soluble cases of the discrete logarithm problems // BIT. 1988. v. 28. №4, 839-851.

[Nest] *Нестеренко Ю. В.,* Частные Ферма и p-адические логарифмы // Труды по дискретной математике. 2002. v. 5. 173-188.

[GP] The Group Properties Wiki, `http://groupprops.subwiki.org/wiki/Exponent_of_direct_product_is_lcm_of_exponents` .

[code] `Kryskov_2013.Rbreve.py`, `http://sdu.bz/7wITxuES` .