Дискретная математика

Модулярная алгебра, криптография, кодирование

Авдошин С.М.
Набебин А.А.

ДМК Пресс
издательство

УДК 519.7
ББК 22.176
А18

Рецензенты:
Калягин В. А. — доктор физико-математических наук, профессор НИУ ВШЭ
Ульянов М. В. — доктор технических наук, профессор,
ведущий научный сотрудник института проблем управления
им. В. А. Трапезникова РАН

Научный редактор:
Захаров В. А. — доктор физико-математических наук,
профессор МГУ им. М. В. Ломоносова

Авдошин С. М., Набебин А. А.
А18 Дискретная математика. Модулярная алгебра, криптография, кодирование. – М.: ДМК Пресс, 2017. – 352 с.: ил.

ISBN 978-5-97060-408-3

Книга содержит необходимые сведения из универсальных и классических алгебр, системы аксиом для основных алгебраических структур (группоид, моноид, полугруппы, группы, частичные порядки, кольца, поля). Описываются основные криптографические алгоритмы. Рассматриваются ставшие классическими помехоустойчивые коды – линейные, циклические, БЧХ. Приводятся алгоритмы проектирования таких кодов.

В основу книги положен многолетний опыт преподавания авторами дисциплины «Дискретная математика» на факультете бизнес-информатика, на факультете компьютерных наук Национального исследовательского университета Высшая школа экономики и на факультете автоматики и вычислительной техники Национального исследовательского университета Московский энергетический институт.

Издание предназначено для студентов бакалавриата, обучающихся по направлениям 09.03.01 «Информатика и вычислительная техника», 09.03.02 «Информационные системы и технологии», 09.03.03 «Прикладная информатика», 09.03.04 «Программная инженерия», а также для ИТ-специалистов и разработчиков программных продуктов.

УДК 519.7
ББК 22.176

ISBN 978-5-97060-408-3

Содержание

Глава 1

Делимость

1.1. Позиционная система счисления

Пусть $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$ есть множество целых чисел, $\mathbb{N} = \{0, 1, 2, 3, ...\}$ есть множество натуральных чисел, $\mathbb{N}_+$ есть множество положительных натуральных чисел.

Сложение, вычитание, умножение, деление целых чисел определяются обычным образом.

Пусть a, b, c есть целые числа. Примем следующие обозначения.

$b \mid a$, b делит a (без остатка).

$b \nmid a$, b не делит a (без остатка).

$a \vdots b$, a делится на b (без остатка).

$\lfloor a/b \rfloor$ есть частное от деления a на b.

$\mathrm{mod}(a,b)$ есть остаток от деления a на b.

Определение. $b \mid a$, если $a = b \cdot q$ при некотором q. *a кратно b*, если $a = b \cdot q$ при некотором q. Число b есть *собственный делитель* a, если $b \mid a$, $b \neq \pm 1$, $b \neq \pm a$.

Замечание. 1. Если a кратно b и b кратно c, то a кратно c.

2. $1 \mid a$, $a \mid a$. Если $a \mid b$ и $b \mid a$, то $a = +b$ или $a = -b$.

3. Если $a \mid b$, $b \mid c$, то $a \mid c$.

4. Если $a \mid b$, то $\forall c \in \mathbb{Z}$ $(a \mid bc)$.

5. Если $k \in \mathbb{Z}$, $k \neq 0$, то $a \mid b \leftrightarrow ka \mid kb$.

6. Если $a \mid b$, $a \mid c$, то $\forall k \in \mathbb{Z}$ $\forall l \in \mathbb{Z}(a \mid (bk + cl))$.

7. Если $a_1 \mid b_1$, ..., $a_n \mid b_n$, то $(a_1 \cdot ... \cdot a_n) \mid (b_1 \cdot ... \cdot b_n)$.

8. Если $a \mid b$, то $a^n \mid b^n$ $\forall n \in \mathbb{Z}$.

9. Если целые $l, ..., n, p, q, ..., s$ делятся на b и удовлетворяют равенству $k + l + ... + n = p + q + ... + s$, то k делится на b. В самом деле, $l = l_1 b$, ..., $n = n_1 b$, $p = p_1 b$, $q = q_1 b$, ..., $s = s_1 b$ и $k = p + q + ... + s - l - ... - n = (p_1 + q_1 + ... + s_1 - l_1 - ... - n_1)b$.

Утверждение (деление с остатком). Пусть $b \in \mathbb{N}_+$. Всякое $a \in \mathbb{Z}$ можно единственным образом представить в виде $a = bq + r$, где $q \in \mathbb{Z}$, $0 \leq r < b$.

Доказательство. Одно такое представление $a = bq + r$, $0 \leq r < b$ можно получить, если bq есть наибольшее кратное для b, не большее a. Если $a = bq_1 + r_1$, $0 \leq r_1 < b$, есть другое такое представление, то вычитание дает $0 = b(q - q_1) + r - r_1$, $r_1 - r = b(q - q_1)$, $r_1 - r$ кратно b. Так как $|r_1 - r| < b$, то $r_1 - r = 0$, $r_1 = r$, $q_1 = q$.

Замечание. 1. Если $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $b \neq 0$, то $\mathrm{mod}(a,b) = a - \lfloor a/b \rfloor \cdot b$.

2. Положим $\mathrm{rest}(a, b) = \begin{cases} \mathrm{mod}(a,b), & \text{если } \mathrm{mod}(a,b) \geq 0, \\ \mathrm{mod}(a,b) + b, & \text{если } \mathrm{mod}(a,b) < 0. \end{cases}$

Пример. Пусть $b = 12$.

$129 = 12 \cdot 10 + 9$, $0 \leq 9 < 12$;
$-65 = 12 \cdot (-5) - 5 + 12 - 12 = 12 \cdot (-6) + 7$, $0 \leq 7 < 12$;
$5 = 12 \cdot 0 + 5$, $0 \leq 5 < 12$;
$-5 = 12 \cdot (-1) + 7$, $0 \leq 7 < 12$;
$204 = 12 \cdot 17 + 0$, $0 \leq 0 < 12$.

Теорема. Для всяких целых $a \geq 0$, $h \geq 2$ при некотором $s \geq 0$ существует единственное представление a в виде

$$a = a_s h^s + a_{s-1} h^{s-1} + \ldots + a_1 h + a_0, \tag{1.1}$$

где $0 \leq a_i \leq h - 1$ $(i = 0, 1, .., s)$, $a_s \neq 0$.

Доказательство. 1. *Существование*. Индукция по a.

Базис. $a = 0$. Тогда $0 = 0 \cdot h^0$, $a_0 = 0$, $s = 0$.

Предположение индукции. Допустим, что теорема верна для всякого натурального $a < n$.

Шаг индукции. Покажем, что теорема верна для $a = n$. По предыдущей теореме $n = hb + r$, $0 \leq r \leq h - 1$, $b < n$. Возможны два случая.

1. $b = 0$. Тогда $n = r$. Представление (1.1) выполняется при $s = 0$, $c_0 = r$.

2. $b \geq 1$. Так как $1 \leq b < n$, то по предположению индукции $b = b_u h^u + b_{u-1} h^{u-1} + \ldots + b_0$ при некотором $u \geq 0$ и $0 \leq b_i \leq h - 1$ $(i = 0, 1, ..., u)$, $b_u \geq 1$. Тогда $n = hb + r = h(b_u h^u + + b_{u-1} h^{u-1} + \ldots + b_0) + r = b_u h^{u+1} + b_{u-1} h^u + \ldots + b_0 h + r$, и мы опять имеем представление в виде (1.1). Существование доказано.

2. *Единственность*. Если

$$a = a_s h^s + a_{s-1} h^{s-1} + \ldots + a_1 h + a_0 = a'_u h^u + \ldots + a'_1 h + a'_0, \tag{1.2}$$

то $a = h(a_s h^{s-1} + \ldots + a_1) + a_0 = h(a'_u h^{u-1} + \ldots + a'_1) + a'_0$. Так как представление $a = hq + r$, $0 \leq r \leq h - 1$, единственно, то $a_0 = a'_0$ и $d = a_s h^{s-1} + \ldots + a_1 = a'_u h^{u-1} + \ldots + a'_1$. Аналогично $a_1 = a'_1$, $a_2 = a'_2$ и т. д. Пусть $s < u$. Тогда $a_0 = a'_0$, $a_1 = a'_1$, ..., $a_s = a'_s$. Удалим одинаковые слагаемые $a_0, a_1 h, ..., a_s h^s$ в (1.2) и получим $a'_u h^u + \ldots + a'_{s+1} h^{s+1} = 0$. Противоречие, ибо $a'_u \geq 1$. Поэтому $s < u$ невозможно. Неравенство $s > u$ тоже невозможно. Остается $s = u$.

Теорема доказана.

Определение. Представление (1.1) называется *представлением числа a* (*в системе счисления*) *по основанию h*. Числа $a_s, a_{s-1}, ..., a_0$ называются *цифрами* числа a по основанию h, и тогда пишут, что по основанию h число

$$a = (a_s a_{s-1} \ldots a_0)_h.$$

Замечание. Представление (1.1) числа a можно рассматривать как многочлен степени s относительно h, который можно использовать для представления

в компьютере сверхбольших чисел (порядка нескольких сот цифр в десятеричном представлении) и для производства целочисленных арифметических операций над ними – сложения, умножения, вычитания, нахождения частного и остатка при их делении, перехода от одной системы счисления к другой и т. д.

Алгоритм вычисления h-ричной записи 10-ричного числа a

ВХОД. Натуральные числа $a > 0$ и $h \geq 2$.
ВЫХОД. h-ричная запись числа $a = (a_t a_{t-1} \ldots a_1 a_0)_h$.
1. $i := 0$.
2. Пока $q \neq 0$, выполняется следующее.
   2.1. $r := \mathrm{mod}(a, h)$, $q := (a - r)/h$.
   2.2. $a := q$, $a_i := r$.
   2.3. $i := i + 1$.
3. Вернуть a.

Пример. Записать 10-ричное число 160 в 7-ричной системе.
Решение. По основанию h число $a_{10} = (a_t a_{t-1} \ldots a_1 a_0)_h$.

$i := 0$, $a := 160$,
$r := \mathrm{mod}(a,h) = \mathrm{mod}(160,7) = 6$, $q := (a - r)/h = (160 - 6)/7 = 22$,
$a_0 := r = 6$, $i := i + 1 = 0 + 1 = 1$; $a := q = 22$,
$r := \mathrm{mod}(a,h) = \mathrm{mod}(22,7) = 1$, $q := (a - r)/h = (22 - 1)/7 = 3$,
$a := q = 3$, $a_1 := r = 1$, $i := i + 1 = 1 + 1 = 2$.
$r := \mathrm{mod}(a,h) = \mathrm{mod}(3,7) = 3$; $q := q := (a - r)/h = (3 - 3)/7 = 0$.
$a := q = 0$, $a_2 := r = 3$, $i := i + 1 = 2 + 1 = 3$.

Ответ. $a = 160_{10} = (a_2 a_1 a_0)_7 = 316_7$.

1.2. Простые числа

Определение. Натуральное число $p \geq 2$ есть *простое число*, если p делится только на 1 и на p, то есть p не имеет собственных делителей. Целое $a > 2$ есть *составное число*, если a имеет собственные делители.

Замечание. 1. Наименьший положительный делитель q целого $a > 1$ есть простое число. В самом деле, пусть $q|a$. Если q есть составное число, то q имеет делитель q_1, для которого $1 < q_1 < q$. Так как $q_1|q$, $q|a$, то $q_1|a$. Противоречие с минимальностью q.

2. Если $q > 1$ есть наименьший делитель составного целого $a > 1$, то $q \leq \sqrt{a}$. В самом деле, так как q есть наименьший делитель a, то $a = qa_1$, $a_1 \geq q$. Перемножим оба выражения и получим $aa_1 \geq qa_1 q$, $a \geq q^2$, $q \leq \sqrt{a}$.

Теорема. Существует бесконечно много простых чисел.

Доказательство. Пусть $p_1, p_2, \ldots, p_k$ есть простые числа. Если число $s = p_1 p_2 \ldots p_k + 1$ простое, то s есть новое простое число. Если s составное, то наименьший больший единицы делитель p для s есть новое простое число. Делитель p не есть один из p_1, $p_2, \ldots, p_k$, иначе $p|s$, $p|(p_1 p_2 \ldots p_k + 1)$, и тогда $p|1$. Противоречие.

Утверждение (число простых чисел). Пусть $\pi(x)$ есть число простых чисел, не превосходящих x. Тогда

1. $\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$.
2. Для $x \geq 17 \pi(x) > \frac{x}{\ln x}$; для $x > 1 \pi(x) < 1{,}25506 \frac{x}{\ln x}$.
3. Для $x \geq 17 \frac{x}{\ln x} < \pi(x) < 1{,}25506 \frac{x}{\ln x}$.

Тест Миллера–Рабина для простоты числа

ВХОД. Нечетное целое $n \geq 3$ и параметр безопасности $t \geq 1$.

ВЫХОД. Ответ «простое» или «составное» на вопрос: «Является ли n простым числом?»

1. Найти s и нечетное r, для которых $n - 1 = 2^s r$.
2. Для i от 1 до t выполнить следующее.
   2.1. Выбрать случайное целое a, $2 \leq a \leq n - 1$.
   2.2. Вычислить $y := a^r \pmod n$.
   2.3. Если $y \neq 1$ и $y \neq n-1$, то выполнить следующее.
   $j := 1$.
   Пока $j \leq s - 1$ и $y \neq n - 1$, выполнить следующее.
   Вычислить $y := y^2 \pmod n$.
   Если $y = 1$, то вернуть «составное».
   $j := j + 1$.
   Если $y \neq n - 1$, то вернуть «составное».
3. Вернуть «простое».

Замечание. Вероятность получить неверный ответ для целого положительного n меньше $(1/4)^t$.

1.3. Факторизация целых чисел

Всякое целое a и p могут иметь общими делителями только 1 или p. В последнем случае a делится на p.

Если произведение нескольких множителей делится на простое p, то хотя бы один множитель делится на p. Допустим противное: все множители не делятся на p. Тогда произведение этих множителей не делится на p. Противоречие. Тогда хотя бы один множитель делится на p.

Теорема (основная теорема арифметики). Всякое целое большее единицы число можно факторизовать (разложить в произведение (положительных) простых сомножителей) единственным образом с точностью до порядка сомножителей.

Доказательство. Пусть целое $a > 1$. Пусть p_1 есть наименьший (положительный) простой делитель a. Тогда $a = p_1 a_1$. Если $a_1 = 1$, нужная факторизация получена. Если $a_1 > 1$, то аналогично получаем $a_1 = p_2 a_2$. Если $a_2 = 1$, нужная факторизация получена. Если $a_2 > 1$, то получаем $a_2 = p_3 a_3$. И так далее. Последовательность a, a_1,

a_2, ... убывает. Поэтому процесс закончится при некотором $a_{n-1} = p_n a_n$, $a_n = 1$. В результате получаем факторизацию $a = p_1 p_2 ... p_n$.

Покажем единственность этой факторизации. Допустим существование другой: $a = q_1 q_2 ... q_s$, и пусть для определенности $s \geq n$. Тогда $p_1 p_2 ... p_n = q_1 q_2 ... q_s$. Правая часть равенства делится на простое p_1. Тогда левая часть равенства делится на q_1 и хотя бы один ее множитель делится на q_1. Пусть $q_1 | p_1$. Тогда $p_1 = q_1$. Сократим равенство на q_1, и пусть $p_2 ... p_n = q_2 ... q_s$. Аналогично получим:

$q_2 = p_2,\ p_3 ... p_n = q_3 ... q_s,$
$q_3 = p_3,\ p_4 ... p_n = q_4 ... q_s,$
...
$q_n = p_n,\ 1 = q_{n+1} ... q_s.$

Поэтому $q_{n+1} = ... = q_s = 1$ и факторизация единственна.

Замечание. 1. Простые сомножители в факторизации могут повторяться. Пусть $p_1 < p_2 < ... < p_k$ есть все различные сомножители в факторизации числа a и a_i есть число вхождений простого p_i в факторизацию. Тогда представление $a = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ есть каноническая факторизация числа a, которая единственна.

2. Если $a = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ есть каноническая факторизация целого a, то

$$d \mid a \leftrightarrow d = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k},$$

где $0 \leq b_1 \leq a_1$, ..., $0 \leq b_k \leq a_k$. Поэтому число a имеет $f(a) = (a_1 + 1)(a_2 + 1) ... (a_k + 1)$ различных делителей.

3. Иногда каноническая факторизация $a = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ включает все отсутствующие простые числа p между 2 и p_k в виде p^0.

4. Распознавание простоты целого числа с 125 цифрами в его десятеричном представлении существующими методами может быть выполнено в несколько минут. Факторизация такого числа на существующих компьютерах потребует миллионы лет компьютерных вычислений, то есть практически неосуществима. С появлением квантовых компьютеров задача факторизации такого числа может быть практически решена за реальное время. Так, например, квантовый компьютер D-Wave канадской фирмы D-Wave Systems способен за секунду решать задачи, на выполнение которых у классического компьютера с одноядерным процессором ушло бы 10 тыс. лет.

Замечание. Если положительное целое n удовлетворяет неравенству $b^{k-1} \leq n < b^k$, то n имеет k цифр по основанию b. Логарифмируем неравенства по основанию b и получаем $k - 1 \leq \log_b n < k$, откуда $k = \lfloor \log_b n \rfloor + 1 = \left\lfloor \frac{\ln n}{\ln b} \right\rfloor + 1$.

1.4. Наибольший общий делитель

Определение. *Общий делитель* од(a, b, ..., l) целых a, b, ..., l есть всякое целое, которое делит каждое из a, b, ..., l.

Пример. Целое 3 есть общий делитель для 18, 24, 36. Целое 6 есть тоже общий делитель для 18, 24, 36.

Определение. *Наибольший общий делитель* нод(a, b, ..., l) или (a, b, ..., l) чисел a, b, ..., l есть наибольший положительный делитель среди всех общих делителей для a, b, ..., l. Полагают, что нод(0, ..., 0) = 0.

Замечание. 1. (a, b, ..., l) есть наибольшее положительное целое, которое делит каждое целое из a, b, ..., l.

2. $d = (a, b)$, если 1) d = од(a, b), 2) если $c|a$, $c|b$, то $c|d$.

Определение. Целые a, b, ..., l *взаимно-просты*, если (a, b, ..., l) = 1.

Замечание. Если целые числа попарно взаимно-просты, то они взаимно-просты. Обратное неверно.

Пример. $(18, 24, 36) = 6, (12, 24, 36) = 12, (14, 28) = 7, (8, 13, 21) = 1, \forall a \neq 0\ ((0,a) = a)$, $\forall a \neq 0\ ((1, a) = 1)$.

Замечание. 1. Если $a = bq + c$, то множество общих делителей для a и b совпадает с множеством общих делителей для b и c. В частности, $(a, b) = (b, c)$.

2. Если $c = 0$ и не все целые a, ..., b равны нулю, то (a, ..., b, c) = (a, ..., b).

Теорема. Если целые $a > 1$, $b > 1$ и их канонические факторизации

$$a = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s},\ b = p_1^{b_1} p_2^{b_2} \dots p_s^{b_s}$$

где p_1, ..., p_s есть все различные простые делители для a или b, то

$$d = (a,b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdot \dots \cdot p_s^{\min(a_s, b_s)}.$$

Доказательство. Пусть $a > 1$, $b > 1$ и p_1, ..., p_s есть множество всех простых чисел, которые делят хотя бы один из a, b. Если простое p из p_1, ..., p_s отсутствует в канонической факторизации a, то добавим к ней множитель p^0. Далее имеем следующее.

1. $d > 0$.
2. Так как $a_1 \geq \min(a_1, b_1)$, ..., $a_s \geq \min(a_s, b_s)$, то $d|a$, $d|b$.
3. Если $h|a$, $h|b$, то $h = p_1^{d_1} p_2^{d_2} \dots p_s^{d_s}$, где

   $d_1 \leq a_1$, $d_1 \leq b_1$, откуда $d_1 \leq \min(a_1, b_1)$,

   ...

   $d_s \leq a_s$, $d_s \leq b_s$, откуда $d_s \leq \min(a_s, b_s)$.

   Тогда $h|d$. Следовательно, $d = (a,b)$.

Замечание. 1. Если $a_1 > 1$, ..., $a_n > 1$,

$$a_1 = p_1^{a_{11}} p_2^{a_{12}} \dots p_s^{a_{1s}},\ a_n = p_1^{a_{n1}} p_2^{a_{n2}} \dots p_s^{a_{ns}},$$

где p_1, ..., p_s есть множество всех различных простых делителей чисел a_1, ..., a_n, то $(a_1, ..., a_n) = p_1^{\min(a_{11}, a_{1s})} \cdot p_2^{\min(a_{n2}, a_{ns})}$.

2. $(a_1, ..., a_{n-1}, a_n) = ((a_1, ..., a_{n-1}), a_n)$.

1.4.1. Алгоритм Евклида вычисления наибольшего общего делителя

Пусть a и b есть натуральные числа и $a \geq b$. Деление с остатком дает следующую последовательность равенств:

$a = bq_1 + r_2,\ 0 < r_2 < b,$
$b = r_2q_2 + r_3,\ 0 < r_3 < r_2,$
$r_2 = r_3q_3 + r_4,\ 0 < r_4 < r_3,$
$r_3 = r_4q_4 + r_5,\ 0 < r_5 < r_4,$
...
$r_{n-2} = r_{n-1}\, q_{n-1} + r_n,$
$r_{n-1} = r_n\, q_n$ (здесь $r_{n+1} = 0$).

Так как последовательность остатков $r_2, r_3, \ldots$ строго убывает, то $r_{n+1} = 0$ при некотором n. Пусть $d = (a, b)$. Тогда из первого равенства получаем, что $d|a$, $d|b$, $d|r_2$, откуда $d = (b, r_2)$, ибо если $d'|b$, $d'|r_2$ для некоторого $d' > d$, то $d'|a$ и $d \neq (a, b)$. Аналогичные рассуждения, примененные к вышенаписанным равенствам, последовательно дают:

$$d = (a, b) = (b, r_2) = (r_2, r_3) = \ldots = (r_{n-1}, r_n) = r_n.$$

Следовательно, $(a, b) = r_n$.

Замечание. Множество общих делителей для a и b совпадает с множеством делителей для $d = (a, b)$.

Алгоритм Евклида вычисления наибольшего общего делителя

ВХОД. Натуральные числа a и b, $a \geq b$.
ВЫХОД. (a, b).
1. Пока $b \neq 0$, выполнять следующее.
   $q := \lfloor a/b \rfloor$, $r := a - qb$, $a := b$, $b := r$.
2. Вернуть a.

Пример. Найти (1050, 231).
$1050 = 231 \cdot 4 + 126$, остаток $r = 126$.
$231 = 126 \cdot 1 + 105$, остаток $r = 105$.
$126 = 105 \cdot 1 + 21$, остаток $r = 21$.
$105 = 21 \cdot 5$, остаток $r = 0$.
$d = (1050, 231) = 21$.

Утверждение. $\forall m \in \mathbb{N}$ $((am, bm) = (a, b)m)$.

Доказательство. Умножим равенства алгоритма Евклида на m и получим $(am, bm) = r_n m$. Так как $(a, b) = r_n$, то $(am, bm) = (a, b)m$.

Замечание. Теорема верна для нескольких чисел.

Утверждение. Если $d = \text{од}(a,b)$, то $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a,b)}{d}$.

Доказательство.

$$(a,b) = \left(\frac{a}{d} \cdot d, \frac{b}{d} \cdot d\right) = \left(\frac{a}{d}, \frac{b}{d}\right)d, \text{ откуда } \left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a,b)}{d}.$$

Следствие. $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1.$

Замечание. Теорема верна для нескольких чисел.

Утверждение. Если $(a, b) = 1$, то $(ac, b) = (c, b)$.

Доказательство. (ac, b) делит ac, b и ac, bc. Тогда (ac, b) делит $(ac, bc) = (a, b)c = c$, то есть (ac, b) делит c. Но (ac, b) делит b. Поэтому(ac, b) делит (c, b).

(c, b) делит c, b и ac, b. Тогда (c, b) делит (ac, b).

(ac, b) и (c, b) делят друг друга. Тогда $(ac, b) = (c, b)$.

Утверждение. Если $(a, b) = 1$ и $b|ac$, то $b|c$.

Доказательство. Из $(a, b) = 1$ следует $(ac, b) = (c, b)$. Так как $b|ac$, то $(c, b) = (ac, b) = b$ делит c.

Теорема. Если каждое из $a_1, ..., a_m$ взаимно-просто с каждым из $b_1, ..., b_n$, то произведение $a_1 \cdot ... \cdot a_m$ взаимно-просто с произведением $b_1 \cdot ... \cdot b_n$.

Доказательство. Пусть $k = 1, 2, ... n$. Тогда

$(a_1, b_k) = 1 \to (a_1a_2, b_k) = (a_2, b_k) = 1.$
$(a_1a_2, b_k) = 1 \to (a_1a_2a_3, b_k) = (a_3, b_k) = 1.$
...
$(a_1a_2 ... a_{n-1}, b_k) = 1 \to (a_1a_2 ... a_{n-1}a_n, b_k) = (a_n, b_k) = 1.$

Пусть $A = a_1 a_2 ... a_n$. Тогда $(A, b_k) = (b_k, A) = 1, k = 1, 2, ..., n$.
Далее

$(b_1, A) = 1 \to (b_1b_2, A) = (b_2, A) = 1.$
$(b_1b_2, A) = 1 \to (b_1b_2b_3, A) = (b_1b_2, A) = 1.$
...
$(b_1...b_{n-1}, A) = 1 \to (b_1...b_{n-1}b_n, A) = (b_1...b_{n-1}, A) = 1.$
$(a_1 \cdot ... \cdot a_m, b_1 \cdot ... \cdot b_n) = 1.$

Замечание. 1. Если $(a, b) = 1$, то $\forall n \in \mathbb{N}\ \forall m \in \mathbb{N}\ ((a^n, b^m) = 1)$.

2. Если для некоторых положительных натуральных n и m $(a^n, b^m) = 1$, то $(a, b) = 1$. В самом деле, если $(a, b) = d$, то $d|a$, $d|b$, $d|a^n$, $d|b^m$, $d|((a^n, b^m))$, $d|1$, $d = 1$.

3. Если p есть простое число, $(a, p^m) \neq 1$, то $(a, p) \neq 1$, $p|a$.

4. Если $(a_1, a_2) = d_2$, $(d_2, a_3) = d_3$, ..., $(d_{n-1}, a_n) = d_n$, то $(a_1, a_2, ..., a_n) = d_n$. В самом деле, множество общих делителей для a_1, a_2 совпадает с множеством делителей для $d_2 = (a_1, a_2)$. Множество общих делителей для d_2, a_3 (множество общих делителей для a_1, a_2, a_3) совпадает с множеством делителей для $d_3 = (d_2, a_3)$. И так далее. Множество общих делителей для a_1, a_2, a_3 совпадает с множеством делителей для $d_n = (d_{n-1}, a_n)$. Так как d_n есть наибольший делитель для d_n, то $(a_1, ..., a_n) = d_n$.

Теорема. $\forall a_1 \in \mathbb{Z} ... \forall a_n \in \mathbb{Z}\ \exists \lambda_1 \in \mathbb{Z} ... \exists \lambda_n \in \mathbb{Z}$ (нод$(a_1, ..., a_n) = \sum_{i=1}^{n} \lambda_i a_i$).

Доказательство. Пусть $S = \{\sum_{i=1}^{n} \mu_i a_i$: все $\mu_i \in \mathbb{Z}\}$. Пусть $d = \sum_{i=1}^{n} \lambda_i a_i$ есть наименьшее положительное целое из S. Покажем, что $d = (a_1, ..., a_n)$. Так как $d \neq 0$, то каждое $a_i = q_i d + r_i$ с $0 \leq r_i < d$. Покажем, что все $r_i = 0$. Пусть для простоты $i = 1$. Допустим противное: $r_1 \neq 0$. Целое $r_1 = a_1 - q_1 d = a_1 - q_1(\lambda_1 a_1 + ... + \lambda_n a_n) = (1 - \lambda_1 q_1)a_1 - q_1\lambda_2 a_2 - - ... - q_1\lambda_n a_n \in S$ и $0 < r_1 < d$. Противоречие с минимальностью d. Следовательно, все $r_i = 0$, $a_i = q_i d$, $d|a_i$, $d =$ од$(a_1, ..., a_n)$.

Если s есть любой другой од$(a_1, ..., a_n)$, то

$a_i = h_i s$, $d = \sum_{i=1}^{n} \lambda_i a_i = \sum_{i=1}^{n} \lambda_i h_i s = s \sum_{i=1}^{n} \lambda_i h_i$, и $s|d$.

Тогда d = нод$(a_1, ..., a_n)$.

Следствие. 1. $\forall a_1 \in \mathbb{Z}\ \forall a_2 \in \mathbb{Z}\ \exists \lambda_1 \in \mathbb{Z}\ \exists \lambda_2 \in \mathbb{Z}\ ((a_1, a_2) = \lambda_1 a_1 + \lambda_2 a_2)$.

2. Если $a_1 \in \mathbb{Z}$, $a_2 \in \mathbb{Z}$ и $1 = (a_1, a_2)$, то $\lambda_1 \in \mathbb{Z}$, $\lambda_2 \in \mathbb{Z}$ $(1 = \lambda_1 a_1 + \lambda_2 a_2)$.

1.4.2. Расширенный алгоритм Евклида вычисления наибольшего общего делителя

Алгоритм Евклида может быть описан следующим образом:

$a = bq_1 + r_2$, $0 < r_2 < b$, $q_1 = \lfloor a/b \rfloor$, $r_2 = a - bq_1$,
$b = r_2 q_2 + r_3$, $0 < r_3 < r_2$, $q_2 = \lfloor b/r_2 \rfloor$, $r_3 = b - r_2 q_2$,
$r_2 = r_3 q_3 + r_4$, $0 < r_4 < r_3$, $q_3 = \lfloor r_2/r_3 \rfloor$, $r_4 = r_2 - r_3 q_3$,
$r_3 = r_4 q_4 + r_5$, $0 < r_5 < r_4$, $q_4 = \lfloor r_3/r_4 \rfloor$, $r_5 = r_3 - r_4 q_4$,
...
$r_{n-2} = r_{n-1} q_{n-1} + r_n$, $q_{n-1} = \lfloor r_{n-2}/r_{n-1} \rfloor$, $r_n = r_{n-2} - r_{n-1} q_{n-1}$,
$r_{n-1} = r_n q_n + r_n$, $q_{n-1} = \lfloor r_{n-2}/r_{n-1} \rfloor$, $r_n = r_{n-2} - r_{n-1} q_{n-1}$,
$r_{n-1} = r_n q_n$ (здесь $r_{n+1} = 0$), $d = r_n$.

Тогда

$r_2 = a - bq_1 = a \cdot 1 + b(-q_1) = aq_1 + bv_1$, $u_1 = 1$, $v_1 = -q_1$,
$r_3 = b - r_2 q_2 = b - (ar_1 + bv_1) = b(1 - v_1) + a(-u_1) = au_2 + bv_2$, $u_2 = 1 - v_1$, $v_2 = -u_1$,
$r_4 = r_2 - r_3 q_3 = (au_1 + bv_1) - (au_2 + bv_2)q_3 = a(u_1 - u_2 q_3) + b(v_1 - v_2 q_3) = au_3 + bv_3$,
$u_3 = u_1 - u_2 q_3$, $v_3 = v_1 - v_2 q_3$,
$r_5 = r_3 - r_4 q_4 = (au_2 + bv_2) - (au_3 + bv_3)q_3 = a(u_2 - u_3 q_4) + b(v_2 - v_3 q_4) = au_4 + bv_4$,
$u_4 = u_2 - u_3 q_4$, $v_4 = v_2 - v_3 q_4$,
...
$d = r_n = r_{n-2} - r_{n-1} q_{n-1} = (au_{n-3} + bv_{n-3}) - (au_{n-2} + bv_{n-2})q_{n-1} =$
$= a(u_{n-3} - u_{n-2} q_{n-1}) + b(v_{n-3} - v_{n-2} q_{n-1}) = au_{n-1} + bv_{n-1}$,
$u_{n-1} = u_{n-3} - u_{n-2} q_{n-1}$, $v_{n-1} = v_{n-3} - v_{n-2} q_{n-1}$.

Получили: $d = r_n$, $u = u_{n-1}$, $v = v_{n-1}$.

Расширенный алгоритм Евклида вычисления d = нод(a,b), $a \geq b$, и чисел u, v, для которых $d = ua + vb$

ВХОД. Натуральные числа a и b, $a \geq b$.
ВЫХОД. d = нод(a,b) и целые u, v, для которых $d = ua + vb$.

1. Если $b = 0$, то $d := a$, $u := 1$, $v := 0$ и вернуть (d, u, v).
2. $u_2 := 1$, $u_1 := 0$, $v_2 := 0$, $v_1 := 1$.
3. Пока $b > 0$, выполнять следующее.
   3.1. $q := \lfloor a/b \rfloor$, $r := a - qb$, $u := u_2 - q\,u_1$, $v := v_2 - q\,v_1$.
   3.2. $a := b$, $b := r$, $u_2 := u_1$, $u_1 := u$, $v_2 := v_1$, $v_1 := v$.
4. $d := a$, $u := u_2$, $v := v_2$, вернуть (d, u, v).

Пример. Найти $d = (a, b)$ и целые u, v, для которых $d = au + bv$.
Целые $a = 5187$, $b = 1520$.
Решение. Вычисления приведены в следующей таблице.

n	q	r	u	v	a	b	u_2	u_1	v_2	v_1
0	–	–	–	–	5187	1520	1	0	0	1
1	3	627	1	–3	1520	627	0	1	1	–3
2	2	266	–2	7	627	266	1	–2	–3	7
3	2	95	5	–17	266	95	2	5	7	–17
4	2	76	–12	41	95	76	5	–12	–17	41
5	1	19	17	–58	76	19	–12	17	41	–58
6	4	0	–80	273	19	0	17	–80	–58	273

Ответ. $d = (a, b) = (3549, 1040) = 19$, $u = 17$, $v = -58$.
Теорема. $\forall s \in \mathbb{N}_+ \; \forall t \in \mathbb{N}_+ \; \forall r \in \mathbb{N}_+$, $s \le t$ (нод(s, t) = нод$(s, t - rs)$).
Доказательство. Если $d|s$, $d|t$, то $d|(t - rs)$. Поэтому всякий од(s, t) есть также од$(s, t - rs)$. Аналогично всякий од$(s, t - rs)$ есть также од(s,t), ибо $t = (t - rs) + rs$. Получено, что множество всех од(s, t) совпадает со множеством всех од$(s, t - rs)$. Следовательно, нод(s, t) = нод$(s, t - rs)$.
Замечание. Эта теорема дает алгоритм вычисления (s, t) последовательным вычитанием меньшего из большего, пока получающиеся два целых числа не совпадут. Эти равные целые есть (s, t).
Теорема. Если t, m, n есть положительные целые, то

$$\text{нод}(t^n - 1, t^m - 1) = t^{\text{нод}(n,m)} - 1.$$

Доказательство. Индукция по max(n, m). Если max$(n, m) = 1$ или $n = m$, то результат тривиален. Иначе допустим $m < n$ и заметим, что

$$(t^n - 1) - t^{n-m}(t^m - 1) = t^{n-m} - 1.$$

Тогда по предыдущей теореме

$$(t^n - 1, t^m - 1) = \left(\underbrace{t^m - 1}_{s}, \underbrace{t^n - 1}_{t}\right) = \left(\underbrace{t^m - 1}_{s}, \underbrace{t^n - 1}_{t} - \underbrace{t^{n-m}}_{r}\left(\underbrace{t^m - 1}_{s}\right)\right) =$$

$$= (t^m - 1, t^{n-m} - 1) = t^{(m,\,n-m)} - 1 = t^{(n,\,m)} - 1.$$

Следствие. При тех же допущениях $(x^{q^n} - x, x^{q^d} - x) = x^{q^{(n,d)}}$.

1.5. Наименьшее общее кратное

Определение. *Общее кратное* ок$(a, b, ..., l)$ целых $a, b, ..., l$ есть всякое целое, которое кратно каждому из $a, b, ..., l$.
Определение. *Наименьшее общее кратное* нок$(a, b, ..., l)$ или $[a, b, ..., l]$ целых $a, b, ..., l$ есть наименьшее неотрицательное целое среди всех общих кратных для $a, b, ..., l$.

Замечание. 1. $[a, b, ..., l]$ есть наименьшее неотрицательное целое, которое делится на каждое целое из $a, b, ..., l$.

2. $d = [a, b]$, если 1) $a|d$, $b|d$, 2) если $a|c$, $b|c$, то $d|c$.

Пример. ок$(18, 21) = 18 \cdot 21 = 378$, ок$(6, 12, 18) = 72$; $[18, 21] = 126$, $[6, 12, 18] = 36$.

Замечание. 1. $[a_1, ..., a_n] = m \leftrightarrow$ 1) $0 < m, m \in \mathbb{Z}$ 2) $a_1|m, ..., a_n|m$, 3) если $0 < M, M \in \mathbb{Z}$ и $a_1|M, ..., a_n|M$, то $m \le M$.

2. Если $a_n = 1$, то $[a_1, ..., a_{n-1}, a_1] = [a_1, ..., a_{n-1}]$.

Утверждение. Если целые $a > 1$, $b > 1$ и их факторизации

$$a = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}, \; b = p_1^{b_1} p_2^{b_2} \dots p_s^{b_s},$$

где $p_1, ..., p_s$ есть все различные простые делители для a или b, то

$$m = [a,b] = p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdot \dots \cdot p_s^{\max(a_s, b_s)}.$$

Доказательство. Пусть $a > 1$, $b > 1$ и $p_1, ..., p_s$ есть все простые числа, которые делят хотя бы одно из a, b. Если простое p из $p_1, ..., p_s$ отсутствует в канонической факторизации a, то добавим к ней множитель p^0. Аналогично для b. Далее имеем следующее.

1. $m > 0$ есть целое число.

2. $a_1 \le \max(a_1, b_1), ..., a_s \le \max(a_s, b_s)$. Поэтому $a_1|m, ..., a_n|m$.

3. Пусть $M > 0$ есть целое число и $a_1|M, ..., a_n|M$. Целое $M = p_1^{l_1} p_2^{l_2} \dots p_s^{l_s} N$ (все $l_i \ge 0$). Так как $a_1|M, ..., a_n|M$, то $a_1 \le l_1$, $b_1 \le l_1, ..., a_s \le l_s$, $b_s \le l_s$, откуда $l_1 \ge \max(a_1, b_1), ..., l_s \ge \max(a_s, b_s)$. Поэтому $m|M$, откуда $m \le M$. Следовательно, m есть наименьшее общее кратное для a и b.

Замечание. 1. Если $a_1 > 1, ..., a_n > 1$,

$$a_1 = p_1^{a_{11}} p_2^{a_{12}} \dots p_s^{a_{1s}}, \dots, a_n = p_1^{a_{n1}} p_2^{a_{n2}} \dots p_s^{a_{ns}},$$

где $p_1, ..., p_s$ есть множество всех различных простых делителей чисел $a_1, ..., a_n$, то

$$[a_1, ..., a_n] = p_1^{\max(a_{11}, \dots, a_{n1})} \cdot \dots \cdot p_s^{\max(a_{1s}, \dots, a_{ns})}.$$

2. $[a_1, ..., a_{n-1}, a_n] = [[a_1, ..., a_{n-1}], a_n]$.

Теорема. Пусть $a \ge 1$, $b \ge 1$ есть натуральные числа, $d = (a, b)$, $m = [a, b]$. Тогда $dm = ab$.

Доказательство. Пусть $a > 1$, $b > 1$ и $a = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}$, $b = p_1^{b_1} p_2^{b_2} \dots p_s^{b_s}$, где $p_1, ..., p_s$ есть все различные простые делители чисел a или b. Если простое p из $p_1, ..., p_s$ отсутствует в канонической факторизации a, то добавим к ней множитель p^0. Аналогично для b. Далее имеем следующее.

$$d = (a,b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdot \dots \cdot p_s^{\min(a_s, b_s)},$$
$$m = [a,b] = p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdot \dots \cdot p_s^{\max(a_s, b_s)},$$
$$\min(a_1, b_1) + \max(a_1, b_1) = a_1 + b_1,$$
$$\dots$$
$$\min(a_s, b_s) + \max(a_s, b_s) = a_s + a_s, \text{ откуда } dm = ab.$$

Следствие. $[a, b] = \dfrac{a \cdot b}{(a,b)}$.

Замечание. 1. Всякое ок$(a, b) = [a, b] \cdot t$ для некоторого натурального t.

2. $[a_1,\ldots,a_n] = \dfrac{a_1 \cdot \ldots \cdot a_n}{(a_1,\ldots,a_n)}$.

3. Наименьшее общее кратное взаимно-простых чисел равно их произведению.

4. Если $m_1|a, \ldots, m_k|a$, то $[m_1, \ldots, m_k]|a$.

Теорема. Пусть натуральные числа $a \geq 2$, $b \geq 2$. Тогда a, b взаимно-просты, если и только если канонические факторизации для a, b не имеют общих простых множителей.

Доказательство. Если $(a, b) = 1$, то канонические факторизации a, b не имеют общих простых множителей, иначе $(a, b) > 1$.

Пусть канонические факторизации для a, b не имеют общих простых множителей. Тогда $a = p_1^{a_1} p_2^{a_2} \ldots p_s^{a_s}$, $b = p_1^{b_1} p_2^{b_2} \ldots p_s^{b_s}$, где $c_i = \min(a_i, b_i) = 0$, $i = 1, 2, \ldots, s$. Поэтому $d = (a,b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdot \ldots \cdot p_s^{\min(a_s, b_s)} = 1$.

Следствие. Если p – простое число, то верно следующее.

1. $p \nmid a \leftrightarrow$ в канонической факторизации a нет множителя с p.
2. $p \nmid a \leftrightarrow (a, p) = 1$.

1.6. Непрерывные (цепные) и подходящие дроби

Пусть c есть вещественное число. Пусть q_1 есть наибольшее целое не больше, чем c. При нецелом c имеем

$$c = q_1 + \frac{1}{c_2}, c_2 > 1.$$

Аналогично

$$c_2 = q_2 + \frac{1}{c_3}, c_3 > 1; c_3 = q_3 + \frac{1}{c_4}, c_3 > 1; \ldots; c_{s-1} = q_{s-1} + \frac{1}{c_s}, c_s > 1.$$

Получили представление c в виде непрерывной (цепной) дроби:

$$c = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cdots + \cfrac{1}{q_{s-1} + \cfrac{1}{c_s}}}}}.$$

Если число c иррационально, то всякое c_s иррационально и дробь продолжается до бесконечности. Если число c рационально, то $c = a/b$ для некоторых целых a, b с $(a, b) = 1$, $b > 0$. Тогда непрерывная дробь будет конечной, и с помощью алгоритма Евклида ее можно получить следующим образом:

$$a = bq_1 + r_2, \frac{a}{b} = q_1 + \frac{r_2}{b} = q_1 + \frac{1}{b/r_2},$$
$$b = r_2 q_2 + r_3, \frac{b}{r_2} = q_2 + \frac{1}{r_2/r_3},$$
$$r_2 = r_3 q_3 + r_4, \frac{r_2}{r_3} = q_3 + \frac{1}{r_3/r_4},$$
$$\ldots$$
$$r_{n-2} = r_{n-1} q_{n-1} + r_n, \frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{1}{r_{n-1}/r_n},$$
$$r_{n-1} = r_n q_n, r_{n+1} = 0, \frac{r_{n-1}}{r_n} = q_n.$$

Тогда непрерывная дробь

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cdots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}.$$

Дроби $\delta_1 = q_1, \delta_2 = q_1 + \frac{1}{q_2}, \delta_3 = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}}$, ... называются *подходящими дробями*.

1.6.1. Вычисление подходящих дробей

δ_s можно получить из δ_{s-1} заменой q_{s-1} в δ_{s-1} на $q_{s-1} + 1/q_s$.

Получим $P_0 = 1$, $Q_0 = 0$. Тогда

$$\delta_1 = \frac{q_1}{1} = \frac{P_1}{Q_1}, \begin{cases} P_1 = q_1, \\ Q_1 = 1, \end{cases} \quad \delta_2 = \delta_1(q_1)\big|_{q_1 := q_1 + 1/q_2},$$
$$\delta_2 = \frac{q_1 + \frac{1}{q_2}}{1} = \frac{q_1 q_2 + 1}{q_2 \cdot 1 + 0} = \frac{q_2 P_1 + P_0}{q_2 Q_1 + Q_0} = \frac{P_2}{Q_2},$$
$$\delta_3 = \frac{P_1\left(q_2 + \frac{1}{q_3}\right) + P_0}{Q_1\left(q_2 + \frac{1}{q_3}\right) + Q_0} = \frac{(P_1 q_2 + P_0) q_3 + P_1}{(Q_1 q_2 + Q_0) q_3 + Q_1} = \frac{q_3 P_2 + P_1}{q_3 Q_2 + Q_1} = \frac{P_3}{Q_3},$$
$$\ldots$$
$$\delta_s = \frac{q_s P_{s-1} + P_{s-2}}{q_s Q_{s-1} + Q_{s-2}} = \frac{P_s}{Q_s},$$
$$\ldots$$

1.6.2. Алгоритм вычисления подходящих дробей

$$P_0 = 1,\ Q_0 = 0,\ P_1 = q_1,\ Q_1 = 1,\ \delta_1 = \frac{P_1}{Q_1},$$

$$\delta_s = \frac{P_s}{Q_s},\ \text{где}\ \begin{cases} P_s = q_s P_{s-1} + P_{s-2} \\ Q_s = q_s Q_{s-1} + Q_{s-2} \end{cases},\quad s = 2, 3, 4, \ldots$$

Пример. Найдем непрерывную дробь для числа 105/38.

$105 = 38 \cdot 2 + 29,\ q_1 = 2,$
$38 = 29 \cdot 1 + 9,\ q_2 = 1,$
$29 = 9 \cdot 3 + 2,\ q_3 = 3,$
$9 = 2 \cdot 4 + 1,\ q_4 = 4,$
$2 = 1 \cdot 2,\ q_5 = 2.$

$$\frac{105}{38} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cfrac{1}{q_5}}}} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{2}}}}.$$

Подходящие дроби. $P_0 = 1$, $Q_0 = 0$, $P_1 = q_1 = 2$, $Q_1 = 1$,

$$\begin{cases} P_0 = 1, P_1 = q_1 = 2, \\ Q_0 = 0, Q_1 = 1, \end{cases} \quad \delta_1 = \frac{P_1}{Q_1} = \frac{2}{1} = 2;$$

$$\begin{cases} P_2 = q_2 P_1 + P_0 = 1 \cdot 2 + 1 = 3, \\ Q_2 = q_2 Q_1 + Q_0 = 1 \cdot 1 + 0 = 1, \end{cases} \quad \delta_2 = \frac{P_2}{Q_2} = \frac{3}{1} = 3;$$

$$\begin{cases} P_3 = q_3 P_2 + P_1 = 3 \cdot 3 + 2 = 11, \\ Q_3 = q_3 Q_2 + Q_1 = 3 \cdot 1 + 1 = 4, \end{cases} \quad \delta_3 = \frac{P_3}{Q_3} = \frac{11}{4};$$

$$\begin{cases} P_4 = q_4 P_3 + P_2 = 4 \cdot 11 + 3 = 47, \\ Q_4 = q_4 Q_3 + Q_2 = 4 \cdot 4 + 1 = 17, \end{cases} \quad \delta_4 = \frac{P_4}{Q_4} = \frac{47}{17};$$

$$\begin{cases} P_5 = q_5 P_4 + P_3 = 2 \cdot 47 + 11 = 105, \\ Q_5 = q_5 Q_4 + Q_3 = 2 \cdot 17 + 4 = 38, \end{cases} \quad \delta_5 = \frac{P_5}{Q_5} = \frac{105}{38}.$$

Теорема. Подходящие дроби δ_s, $s > 1$, несократимы.
Доказательство.

$$\delta_s - \delta_{s-1} = \frac{P_s}{Q_s} - \frac{P_{s-1}}{Q_{s-1}} = \frac{P_s Q_{s-1} - Q_s P_{s-1}}{Q_s Q_{s-1}} = \frac{h_s}{Q_s Q_{s-1}};$$

$$\begin{aligned} h_s &= P_s Q_{s-1} - Q_s P_{s-1} = \\ &= (q_s P_{s-1} + P_{s-2}) Q_{s-1} - (q_s Q_{s-1} + Q_{s-2}) P_{s-1} = \\ &= q_s P_{s-1} Q_{s-1} + P_{s-2} Q_{s-1} - q_s Q_{s-1} P_{s-1} - Q_{s-2} P_{s-1} = \\ &= P_{s-2} Q_{s-1} - Q_{s-2} P_{s-1} = -(P_{s-1} Q_{s-2} - Q_{s-1} P_{s-2}) = -h_{s-1}. \end{aligned}$$

Аналогично получаем

$h_s = (-1)h_{s-1} = (-1)^2 h_{s-2} = (-1)^3 h_{s-3} = \ldots = (-1)^{s-1} h_{s-(s-1)} = (-1)^{s-1} h_1 =$
$= (-1)^{s-1} (P_1Q_0 - Q_1P_0) = (-1)^{s-1} (q_1 \cdot 0 - 1 \cdot 1) = (-1)^{s-1} \cdot (-1) = (-1)^s.$

Тогда

$$P_s Q_{s-1} - Q_s P_{s-1} = (-1)^s, \; s > 1, \tag{1.3}$$
$$\delta_s - \delta_{s-1} = (-1)^s/(Q_s Q_{s-1}), \; s > 1. \tag{1.4}$$

Так как (P_s, Q_s) делит P_s, Q_s и левую часть в (1.3), то (P_s, Q_s) делит правую часть в (1.3). Поэтому $(P_s, Q_s) = 1$. Следовательно, подходящие дроби $\delta_s = P_s/Q_s$, $s > 1$, несократимы.

Замечание. Если c есть вещественное число, $s \geq 2$, $c \neq \delta_s$ то по (1.4) c лежит между δ_{s-1}, δ_s и $|c - \delta_{s-1}| \leq |\delta_s - \delta_{s-1}| \leq 1/(Q_s Q_{s-1})$.