

# Дискретная математика

## *Модулярная алгебра, криптография, кодирование*



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

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

ISBN 978-5-97060-408-3

© Авдошин С. М., Набебин А. А., 2016  
© Оформление, издание, ДМК Пресс, 2017

# Содержание

<b>Предисловие</b> .....	<b>11</b>
<b>Введение</b> .....	<b>13</b>
1. Множество .....	13
2. Функция .....	14
3. Отношение .....	16
4. Отношение эквивалентности .....	17
5. Каноническое разложение функции.....	18
6. Мощность множества. Счетные и несчетные множества.....	19
7. Мощность континуума .....	20
8. Кардинальные числа. Сравнение мощностей.....	21
<b>Часть I. МОДУЛЯРНАЯ АЛГЕБРА</b> .....	<b>25</b>
<b>Глава 1. Делимость</b> .....	<b>26</b>
1.1. Позиционная система счисления .....	26
1.2. Простые числа .....	28
1.3. Факторизация целых чисел.....	29
1.4. Наибольший общий делитель.....	30
1.4.1. Алгоритм Евклида вычисления наибольшего общего делителя.....	31
1.4.2. Расширенный алгоритм Евклида вычисления наибольшего общего делителя .....	34
1.5. Наименьшее общее кратное.....	35
1.6. Непрерывные (цепные) и подходящие дроби.....	37
1.6.1. Вычисление подходящих дробей.....	38
1.6.2. Алгоритм вычисления подходящих дробей .....	39
<b>Глава 2. Функции Мебиуса и Эйлера</b> .....	<b>41</b>
2.1. Функции $\lfloor x \rfloor$ , $ x $ , $\{x\}$ для вещественного $x$ .....	41
2.2. Мультипликативные функции .....	42
2.3. Функция и формула обращения Мебиуса .....	43
2.4. Функция Эйлера .....	47
<b>Глава 3. Сравнения</b> .....	<b>49</b>
3.1. Сравнение целых чисел.....	49
3.2. Свойства сравнений .....	49
3.3. Полная система вычетов.....	51

Операции над классами .....	51
3.4. Приведенная система вычетов.....	53
3.5. Теоремы Эйлера и Ферма.....	54
3.6. Классы целых чисел по модулю $m$ , взаимно простых с модулем $m$ .....	54
3.7. Модулярные арифметические операции .....	55
3.7.1. Алгоритм вычисления мультипликативно обратного элемента $a^{-1} \pmod{n}$ в $\mathbb{Z}_n$ .....	56
3.7.2. Алгоритм вычисления модулярной степени в $\mathbb{Z}_n$ .....	56
3.7.3. Алгоритм вычисления генератора мультипликативной циклической группы $\mathbb{Z}_p^*$ при простом $p$ (перебор).....	57
<b>Глава 4. Сравнения с одной переменной.....</b>	<b>58</b>
4.1. Решение сравнения с переменными .....	58
4.2. Сравнения первой степени .....	60
4.3. Система сравнений первой степени.....	61
4.3.1. Попарно взаимно-простые модули.....	61
4.3.2. Алгоритм Гаусса для системы сравнений $x \equiv c_1 \pmod{m_1}, \dots,$ $x \equiv c_k \pmod{m_k}$ с попарно взаимно-простыми модулями .....	62
4.3.3. Произвольные модули .....	63
4.4. Сравнения любой степени с простым модулем .....	64
4.5. Сравнения произвольной степени по составному модулю .....	65
Алгоритм решения сравнения $f(x) \equiv 0 \pmod{p^\alpha}$ .....	68
<b>Глава 5. Сравнения второй степени .....</b>	<b>69</b>
5.1. Квадратичные вычеты по простому модулю .....	69
5.2. Символ Лежандра .....	70
5.3. Символ Якоби.....	74
Алгоритм вычисления символа Якоби (и символа Лежандра) $JACOBI(a, n)$ .....	76
5.4. Квадратичные вычеты по составному модулю .....	77
<b>Глава 6. Примитивные корни и индексы.....</b>	<b>80</b>
6.1. Экспонента, примитивные корни, индексы .....	80
6.1.1. Число классов вычетов данной экспоненты.....	82
6.1.2. Индексы (дискретные логарифмы).....	83
6.2. Примитивные корни по модулям $p^\alpha$ и $2p^\alpha$ .....	83
6.3. Вычисление примитивных корней по модулям $p^\alpha$ и $2p^\alpha$ .....	87
6.4. Индексы по модулям $p^\alpha$ и $2p^\alpha$ .....	88
6.5. Индексы и вычеты .....	88
6.6. Индексы по модулю $2^\alpha$ .....	89
6.7. Индексы по любому составному модулю .....	91

<b>Глава 7. Универсальные алгебры.....</b>	<b>93</b>
7.1. Алгебры, подалгебры, гомоморфизм алгебр.....	93
7.2. Конгруэнции .....	96
<b>Глава 8. Абстрактная алгебра .....</b>	<b>99</b>
8.1. Полугруппы.....	99
8.2. Циклические полугруппы .....	101
8.3. Группы.....	103
8.3.1. Циклические группы .....	107
8.3.2. Смежные классы. Разложение группы по подгруппе .....	107
8.3.3. Конечные группы и теорема Лагранжа .....	109
8.3.4. Конечные циклические группы .....	109
8.3.5. Алгоритм вычисления всех подгрупп конечной циклической группы.....	111
8.4. Нормальные подгруппы, фактор-группы, теорема о гомоморфизме групп.....	111
8.5. Кольцо.....	114
8.6. Поле.....	117
8.7. Полиномиальные кольца.....	120
8.8. Идеал кольца.....	121
8.8.1. Главный идеал.....	122
8.8.2. Разностное кольцо (кольцо классов вычетов). Сравнения.....	122
8.9. Линейное векторное пространство .....	124
8.10. Булева алгебра .....	126
8.11. Решетка.....	126
<b>Глава 9. Конечные поля .....</b>	<b>128</b>
9.1. Представление конечного поля множеством классов вычетов по модулю неприводимого полинома.....	128
9.2. Поле разложения полинома $x^{p^m} - x$ .....	130
9.3. Циклическость мультипликативной группы поля.....	130
9.4. Задание поля корнем неприводимого полинома .....	131
9.5. Строение конечных полей.....	133
9.5.1. Минимальный полином .....	136
9.5.2. Вычисление минимального полинома .....	137
9.5.3. Подполя конечного поля .....	139
9.5.4. Круговые полиномы.....	142
9.5.5. Алгоритм факторизации полинома $x^{p^m-1} - 1$ на круговые полиномы из $GF(q)$ .....	144
9.6. Изоморфизм полей Галуа.....	145
9.7. Автоморфизмы поля Галуа .....	146

9.8. Основные алгоритмы для конечных полей.....	147
9.8.1. Алгоритм Евклида для полиномов из $\mathbb{Z}_p[x]$ .....	149
9.8.2. Расширенный алгоритм Евклида для полиномов из $\mathbb{Z}_p[x]$ .....	150
9.8.3. Мультипликативный обратный элемент в $\mathbb{F}_{p^m}$ .....	153
9.8.4. Модулярная степень в $\mathbb{F}_{p^m}$ .....	153
9.8.5. Тестирование полинома из $\mathbb{Z}_p[x]$ на неприводимость .....	153
9.8.6. Порождение случайного неприводимого полинома над $\mathbb{Z}_p$ .....	153
9.8.7. Тестирование неприводимого полинома на примитивность.....	154
9.8.8. Порождение случайного нормированного примитивного полинома над $\mathbb{Z}_p$ .....	154
9.8.9. Вычисление порядка элемента конечной группы (метод Гаусса) .....	154
9.8.10. Вычисление генератора конечной циклической группы (метод Гаусса).....	154

## **Часть II. КРИПТОГРАФИЯ..... 156**

### **Глава 10. Модулярная алгебра в криптографии..... 157**

10.1. Криптография и ее цели .....	157
10.1.1. Хэш-функция .....	160
10.1.2. Алгоритм MASH-1 .....	161
10.2. Проблема факторизации целых чисел.....	162
10.2.1. $\rho$ -алгоритм Полларда факторизации целых чисел .....	162
10.2.2. $(p - 1)$ -алгоритм Полларда факторизации целых чисел .....	163
10.2.3. Алгоритм квадрат-решета факторизации целых чисел.....	164
10.3. Проблема RSA.....	165
10.4. Проблема квадратичного вычета.....	166
10.4.1. Алгоритм вычисления дискретного квадратного корня по простому модулю $p$ .....	166
10.4.2. Алгоритм вычисления дискретного квадратного корня по простому модулю $p$ , где $p \equiv 3 \pmod{4}$ .....	167
10.4.3. Алгоритм вычисления дискретного квадратного корня по простому модулю $p$ , где $p \equiv 5 \pmod{8}$ .....	167
10.4.4. Алгоритм вычисления дискретного квадратного корня по простому модулю $p$ при большом $s$ .....	167
10.4.5. Алгоритм вычисления дискретного квадратного корня по модулю $n = p \cdot q$ , где $p$ и $q$ есть простые числа.....	167
10.5. Проблема дискретного логарифма .....	168
10.5.1. Алгоритм «малый шаг – большой шаг» вычисления дискретного логарифма.....	168
10.5.2. $\rho$ -алгоритм Полларда вычисления дискретного логарифма .....	169
10.5.3. Алгоритм Полига-Хеллмана вычисления дискретного логарифма .....	171

10.6. Проблема подмножества суммы .....	172
10.6.1. Наивный (переборный) алгоритм решения проблемы суммы.....	172
10.6.2. Алгоритм «встреча посередине» решения проблемы подмножества суммы.....	172
10.7. Проблема факторизации полиномов над конечным полем .....	173
10.7.1. Бесквадратная факторизация.....	173
10.7.2. Q-матричный алгоритм Берлекампа .....	174
10.8. Криптосистема RSA.....	175
10.8.1. Шифросистема RSA .....	175
10.8.2. Электронная цифровая подпись RSA с использованием хэш-функции .....	177
10.8.3. Электронная цифровая подпись RSA с извлечением сообщения .....	179
10.9. Криптосистема Эль-Гамала.....	180
10.9.1. Шифросистема Эль-Гамала над числовым полем Галуа $GF(p)$ .....	180
10.9.2. Электронная цифровая подпись Эль-Гамала над числовым полем Галуа $GF(p)$ .....	182
10.9.3. Шифросистема Эль-Гамала над полиномиальным полем Галуа $GF(p^m)$ .....	184
10.9.4. Электронная цифровая подпись Эль-Гамала над полиномиальным полем Галуа $GF(p^m)$ .....	187
10.10. Электронная цифровая подпись DSA.....	189
10.11. Криптографическая система Рабина .....	192
10.11.1. Шифросистема Рабина.....	192
10.11.2. Электронная цифровая подпись Рабина с извлечением сообщения.....	194
10.11.3. Модифицированная цифровая подпись Рабина с извлечением сообщения.....	195
10.12. Рюкзачная схема шифрования Меркле–Хеллмана.....	198
10.13. Рюкзачная схема шифрования Хора–Ривеста.....	199
10.14. Вероятностные схемы шифрования с открытым ключом.....	203
10.14.1. Вероятностная схема шифрования Голдвассер–Микали .....	204
10.14.2. Вероятностная схема шифрования Блюма–Голдвассер.....	206
10.15. Электронная цифровая подпись Фейге–Фиат–Шамира .....	208
10.16. Электронная цифровая подпись GQ.....	210
10.17. Электронная цифровая подпись Шнорра с хэш-функцией .....	211
10.18. Электронная цифровая подпись Ниберга–Рюппеля с извлечением сообщения.....	213

<b>Глава 11. Криптография на эллиптических кривых над конечными полями .....</b>	<b>215</b>
11.1. Эллиптические кривые .....	215

11.2. Эллиптические кривые над полем вещественных чисел .....	216
11.3. Эллиптические кривые в конечных полях.....	218
11.4. Сложение точек эллиптической кривой $E(F) \ y^2 = x^3 + ax + b$ над полем $F$ характеристики $\text{char}(F) > 3$ .....	219
11.5. Сложение точек эллиптической кривой $E(F) \ y^2 = x^3 + ax^2 + bx + c$ с над полем $F$ характеристики $\text{char}(F) = 3$ .....	220
11.6. Сложение точек суперсингулярной эллиптической кривой $E(F) \ y^2 + cy = x^3 + ax + b$ над полем $F$ характеристики $\text{char}(F) = 2$ .....	222
11.7. Сложение точек несуперсингулярной эллиптической кривой $E(F) \ y^2 + xy = x^3 + ax^2 + b$ над полем $F$ характеристики $\text{char}(F) = 2$ .....	224
11.8. Вычисление $k \cdot P$ .....	226
11.9. Порядок группы точек эллиптической кривой .....	226
11.9.1. Алгоритм вычисления порядка элемента группы точек эллиптической кривой (метод Гаусса) .....	228
11.9.2. Алгоритм вычисления генератора циклической группы точек эллиптической кривой (метод Гаусса) .....	228
11.10. Криптосистемы на эллиптических кривых над числовым конечным полем .....	229
11.10.1. Шифросистема Эль-Гамала на эллиптических кривых над числовым конечным полем.....	229
11.10.2. Электронная цифровая подпись (ЭЦП) Эль-Гамала на эллиптических кривых над числовым конечным полем .....	232
<b>Глава 12. Шифросистема NTRU на конечных полиномиальных кольцах.....</b>	<b>235</b>
12.1. Проблема кратчайшего вектора в целочисленной решетке .....	235
12.2. Шифросистема NTRU .....	236
<b>Глава 13. Блочные и потоковые шифры.....</b>	<b>241</b>
13.1. Блочный шифр RC5-S.....	241
13.2. Потоковые шифры.....	245
13.2.1. Линейный регистр сдвига с обратной связью.....	245
13.2.2. Расшифровка линейного регистра сдвига .....	247
<b>Часть III. КОДИРОВАНИЕ .....</b>	<b>250</b>
<b>Глава 14. Линейные коды .....</b>	<b>251</b>
14.1. Линейные пространства над полями Галуа.....	251
14.2. Расстояние Хэмминга.....	252
14.3. Порождающая и проверочная матрицы.....	253
14.4. Декодирование в ближайшее кодовое слово.....	255



14.5. Расстояние и корректирующая способность кода.....	256
14.6. Каноническая форма базисных матриц систематического кода.....	256
14.6.1. Каноническая проверочная матрица .....	256
14.6.2. Каноническая кодирующая матрица .....	257
14.6.3. Алгоритм систематизации несистематического линейного кода.....	260
14.7. Декодирование линейного кода (декодер).....	261
14.8. Бинарный код Хэмминга.....	263
<b>Глава 15. Циклические коды .....</b>	<b>266</b>
15.1. Порождающая и проверочная матрицы циклического кода .....	266
15.2. Канонические порождающая и проверочная матрицы циклического кода .....	268
15.3. Систематический кодер циклического кода.....	270
<b>Глава 16. Коды Боуза–Чоудхури–Хоквингема (коды БЧХ) .....</b>	<b>271</b>
16.1. Построение кодов БЧХ.....	271
16.2. Декодер Питерсона–Горенштейна–Цирлера .....	276
16.3. Алгоритм Питерсона–Горенштейна–Цирлера БЧХ-кода с исправлением $t$ и менее ошибок .....	281
<b>Глава 17. Коды сжатия информации .....</b>	<b>298</b>
17.1. Алфавитное кодирование.....	298
17.2. Кодирование с минимальной избыточностью.....	299
17.3. Алгоритм Фано построения разделимой префиксной схемы алфавитного кодирования, близкого к оптимальному .....	300
17.4. Оптимальное кодирование .....	301
17.5. Алгоритм Хаффмана оптимальной разделимой префиксной схемы алфавитного кодирования .....	303
17.6. Кодер и декодер Прюфера для деревьев.....	309
<b>Глава 18. Основы теории информации .....</b>	<b>311</b>
18.1. Количество информации и энтропия .....	311
18.1.1. Равновероятность знаков алфавита .....	311
18.1.2. Разновероятность знаков алфавита. Формулы Шеннона .....	313
18.2. Свойства энтропии .....	313
18.3. Энтропия при непрерывном сообщении .....	316
18.4. Условная энтропия .....	319
18.5. Взаимная энтропия .....	326

<b>Приложения .....</b>	<b>327</b>
1. Множества, функции, отношения .....	327
2. Модулярная алгебра .....	334
3. Криптография .....	341
4. Кодирование .....	342
5. Информация и энтропия .....	345
<b>Литература.....</b>	<b>347</b>
<b>Обозначения.....</b>	<b>349</b>

## 1.1. Позиционная система счисления

Пусть  $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$  есть множество целых чисел,  $\mathbb{N} = \{0, 1, 2, 3, \dots\}$  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).

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

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

$\text{mod}(a, b)$  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  $a_1 \mid b_1, \dots, a_n \mid b_n$ , то  $(a_1 \cdot \dots \cdot a_n) \mid (b_1 \cdot \dots \cdot b_n)$ .

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

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

**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  $\text{mod}(a, b) = a - \lfloor a/b \rfloor \cdot b$ .

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

**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

$$a = a_s h^s + a_{s-1} h^{s-1} + \dots + a_1 h + a_0, \quad (1.1)$$

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

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

2. *Единственность.* Если

$$a = a_s h^s + a_{s-1} h^{s-1} + \dots + a_1 h + a_0 = a'_u h^u + \dots + a'_1 h + a'_0, \quad (1.2)$$

то  $a = h(a_s h^{s-1} + \dots + a_1) + a_0 = h(a'_u h^{u-1} + \dots + a'_1) + a'_0$ . Так как представление  $a = hq + r, 0 \leq r < h - 1$ , единственно, то  $a_0 = a'_0$  и  $d = a_s h^{s-1} + \dots + a_1 = a'_u h^{u-1} + \dots + a'_1$ . Аналогично  $a_1 = a'_1, a_2 = a'_2$  и т. д. Пусть  $s < u$ . Тогда  $a_0 = a'_0, a_1 = a'_1, \dots, a_s = a'_s$ . Удалим одинаковые слагаемые  $a_0, a_1 h, \dots, a_s h^s$  в (1.2) и получим  $a'_u h^u + \dots + a'_{s+1} h^{s+1} = 0$ . 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  $a_s, a_{s-1}, \dots, a_0$  называются *цифрами* числа  $a$  по основанию  $h$ , и тогда пишут, что по основанию  $h$  число

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

**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 десятичном 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  $a = (a_t a_{t-1} \dots a_1 a_0)_h$ .

1.  $i := 0$ .
2. Пока  $q \neq 0$ , выполняется следующее.
  - 2.1.  $r := \text{mod}(a, h)$ ,  $q := (a - r)/h$ .
  - 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  $a_{10} = (a_t a_{t-1} \dots a_1 a_0)_h$ .

$i := 0$ ,  $a := 160$ ,

$r := \text{mod}(a, h) = \text{mod}(160, 7) = 6$ ,  $q := (a - r)/h = (160 - 6)/7 = 22$ ,

$a_0 := r = 6$ ,  $i := i + 1 = 0 + 1 = 1$ ;  $a := q = 22$ ,

$r := \text{mod}(a, h) = \text{mod}(22, 7) = 1$ ,  $q := (a - r)/h = (22 - 1)/7 = 3$ ,

$a := q = 3$ ,  $a_1 := r = 1$ ,  $i := i + 1 = 1 + 1 = 2$ .

$r := \text{mod}(a, h) = \text{mod}(3, 7) = 3$ ;  $q := q := (a - r)/h = (3 - 3)/7 = 0$ .

$a := q = 0$ ,  $a_2 := r = 3$ ,  $i := i + 1 = 2 + 1 = 3$ .

*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  $aa_1 \geq qa_1q$ ,  $a \geq q^2$ ,  $q \leq \sqrt{a}$ .

**Теорема.** Существует бесконечно много простых чисел.

**Доказательство.** Пусть  $p_1, p_2, \dots, p_k$  есть простые числа. Если число  $s = p_1 p_2 \dots p_k + 1$  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  $p_1, p_2, \dots, p_k$ , иначе  $p|s$ ,  $p|(p_1 p_2 \dots p_k + 1)$ , и тогда  $p|1$ . Противоречие.

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

1.  $\lim_{x \rightarrow \infty} \frac{\pi(x)}{x / \ln x} = 1$ .
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  $a, a_1,$

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

Покажем единственность этой факторизации. Допустим существование другой:  $a = q_1 q_2 \dots q_s$  и пусть для определенности  $s \geq n$ . Тогда  $p_1 p_2 \dots p_n = q_1 q_2 \dots q_s$ . 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  $p_2 \dots p_n = q_2 \dots q_s$ . Аналогично получим:

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

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

**Замечание.** 1. Простые множители в факторизации могут повторяться. Пусть  $p_1 < p_2 < \dots < p_k$  есть все различные множители 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

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

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

$$b \text{ и получаем } k - 1 \leq \log_b n < k, \text{ откуда } k = \lfloor \log_b n \rfloor + 1 = \left\lfloor \frac{\ln n}{\ln b} \right\rfloor + 1.$$

## 1.4. Наибольший общий делитель

**Определение.** *Общий делитель*  $\text{од}(a, b, \dots, l)$  целых  $a, b, \dots, l$  есть всякое целое, которое делит каждое из  $a, b, \dots, l$ .

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

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

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

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

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

**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  $a, \dots, b$  равны нулю, то  $(a, \dots, b, c) = (a, \dots, b)$ .

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

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

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

1.  $d > 0$ .

2. Так как  $a_1 \geq \min(a_1, b_1), \dots, a_s \geq \min(a_s, b_s)$ , 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

$$d_1 \leq a_1, d_1 \leq b_1, \text{ откуда } d_1 \leq \min(a_1, b_1),$$

...

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

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

**Замечание.** 1. Если  $a_1 > 1, \dots, a_n > 1$ ,

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

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

$$(a_1, \dots, a_n) = p_1^{\min(a_{11}, a_{1s})} \cdot p_2^{\min(a_{n2}, a_{ns})}.$$

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

### 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:



$$\begin{aligned}
a &= bq_1 + r_2, & 0 < r_2 < b, \\
b &= r_2q_2 + r_3, & 0 < r_3 < r_2, \\
r_2 &= r_3q_3 + r_4, & 0 < r_4 < r_3, \\
r_3 &= r_4q_4 + r_5, & 0 < r_5 < r_4, \\
&\dots \\
r_{n-2} &= r_{n-1}q_{n-1} + r_n, \\
r_{n-1} &= r_nq_n \text{ (здесь } r_{n+1} = 0\text{)}.
\end{aligned}$$

Так как последовательность остатков  $r_2, r_3, \dots$  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:

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

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  $(1050, 231)$ .

$$1050 = 231 \cdot 4 + 126, \text{ остаток } r = 126.$$

$$231 = 126 \cdot 1 + 105, \text{ остаток } r = 105.$$

$$126 = 105 \cdot 1 + 21, \text{ остаток } r = 21.$$

$$105 = 21 \cdot 5, \text{ остаток } r = 0.$$

$$d = (1050, 231) = 21.$$

**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  $a_1, \dots, a_m$  взаимно-просто с каждым из  $b_1, \dots, b_n$ , то произведение  $a_1 \cdot \dots \cdot a_m$  взаимно-просто с произведением  $b_1 \cdot \dots \cdot b_n$ .

**Доказательство.** Пусть  $k = 1, 2, \dots, n$ . Тогда

$$(a_1, b_k) = 1 \rightarrow (a_1 a_2, b_k) = (a_2, b_k) = 1.$$

$$(a_1 a_2, b_k) = 1 \rightarrow (a_1 a_2 a_3, b_k) = (a_3, b_k) = 1.$$

...

$$(a_1 a_2 \dots a_{n-1}, b_k) = 1 \rightarrow (a_1 a_2 \dots a_{n-1} a_n, b_k) = (a_n, b_k) = 1.$$

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

Далее

$$(b_1, A) = 1 \rightarrow (b_1 b_2, A) = (b_2, A) = 1.$$

$$(b_1 b_2, A) = 1 \rightarrow (b_1 b_2 b_3, A) = (b_3, A) = 1.$$

...

$$(b_1 \dots b_{n-1}, A) = 1 \rightarrow (b_1 \dots b_{n-1} b_n, A) = (b_n, A) = 1.$$

$$(a_1 \dots a_m, b_1 \dots b_n) = 1.$$

**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  $(a_1, a_2) = d_2, (d_2, a_3) = d_3, \dots, (d_{n-1}, a_n) = d_n$ , то  $(a_1, a_2, \dots, a_n) = d_n$ . 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  $(a_1, \dots, a_n) = d_n$ .

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

**Доказательство.** Пусть  $S = \{\sum_{i=1}^n \mu_i a_i; \text{ все } \mu_i \in \mathbb{Z}\}$ . Пусть  $d = \sum_{i=1}^n \lambda_i a_i$  есть наименьшее положительное целое из  $S$ . Покажем, что  $d = (a_1, \dots, a_n)$ . 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  $r_1 = a_1 - q_1 d = a_1 - q_1(\lambda_1 a_1 + \dots + \lambda_n a_n) = (1 - \lambda_1 q_1) a_1 - q_1 \lambda_2 a_2 - \dots - q_1 \lambda_n a_n \in S$  и  $0 < r_1 < d$ . Противоречие с минимальностью  $d$ . Следовательно, все  $r_i = 0, a_i = q_i d, d|a_i, d = \text{од}(a_1, \dots, a_n)$ .

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

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

Тогда  $d = \text{нод}(a_1, \dots, a_n)$ .

**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:

$$\begin{aligned} a &= bq_1 + r_2, 0 < r_2 < b, q_1 = \lfloor a/b \rfloor, r_2 = a - bq_1, \\ b &= r_2q_2 + r_3, 0 < r_3 < r_2, q_2 = \lfloor b/r_2 \rfloor, r_3 = b - r_2q_2, \\ r_2 &= r_3q_3 + r_4, 0 < r_4 < r_3, q_3 = \lfloor r_2/r_3 \rfloor, r_4 = r_2 - r_3q_3, \\ r_3 &= r_4q_4 + r_5, 0 < r_5 < r_4, q_4 = \lfloor r_3/r_4 \rfloor, r_5 = r_3 - r_4q_4, \\ &\dots \end{aligned}$$

$$\begin{aligned} r_{n-2} &= r_{n-1}q_{n-1} + r_n, q_{n-1} = \lfloor r_{n-2}/r_{n-1} \rfloor, r_n = r_{n-2} - r_{n-1}q_{n-1}, \\ r_{n-1} &= r_nq_n + r_{n+1}, q_n = \lfloor r_{n-1}/r_n \rfloor, r_{n+1} = r_{n-1} - r_nq_n, \\ r_{n+1} &= r_nq_{n+1} \text{ (здесь } r_{n+1} = 0), d = r_n. \end{aligned}$$

Тогда

$$\begin{aligned} r_2 &= a - bq_1 = a \cdot 1 + b(-q_1) = aq_1 + bv_1, u_1 = 1, v_1 = -q_1, \\ r_3 &= b - r_2q_2 = b - (aq_1 + bv_1)q_2 = b(1 - v_1q_2) + a(-u_1q_2) = au_2 + bv_2, u_2 = 1 - v_1q_2, v_2 = -u_1q_2, \\ r_4 &= r_2 - r_3q_3 = (au_1 + bv_1) - (au_2 + bv_2)q_3 = a(u_1 - u_2q_3) + b(v_1 - v_2q_3) = au_3 + bv_3, \\ &u_3 = u_1 - u_2q_3, v_3 = v_1 - v_2q_3, \\ r_5 &= r_3 - r_4q_4 = (au_2 + bv_2) - (au_3 + bv_3)q_4 = a(u_2 - u_3q_4) + b(v_2 - v_3q_4) = au_4 + bv_4, \\ &u_4 = u_2 - u_3q_4, v_4 = v_2 - v_3q_4, \\ &\dots \end{aligned}$$

$$\begin{aligned} d = r_n &= r_{n-2} - r_{n-1}q_{n-1} = (au_{n-3} + bv_{n-3}) - (au_{n-2} + bv_{n-2})q_{n-1} = \\ &= a(u_{n-3} - u_{n-2}q_{n-1}) + b(v_{n-3} - v_{n-2}q_{n-1}) = au_{n-1} + bv_{n-1}, \\ &u_{n-1} = u_{n-3} - u_{n-2}q_{n-1}, v_{n-1} = v_{n-3} - v_{n-2}q_{n-1}. \end{aligned}$$

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

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

**ВХОД.** Натуральные числа  $a$  и  $b, a \geq b$ .

**ВЫХОД.**  $d = \text{нод}(a, b)$  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.**  $\forall s \in \mathbb{N}_+ \forall t \in \mathbb{N}_+ \forall r \in \mathbb{N}_+, s \leq t$  (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

$$\begin{aligned} (t^n - 1, t^m - 1) &= \left( \underbrace{t^m - 1}_s, \underbrace{t^n - 1}_t \right) = \left( \underbrace{t^m - 1}_s, \underbrace{t^n - 1}_t - \underbrace{t^{n-m}}_r \left( \underbrace{t^m - 1}_s \right) \right) = \\ &= (t^m - 1, t^{n-m} - 1) = t^{(n, m)} - 1. \end{aligned}$$

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

## 1.5. Наименьшее общее кратное

**Определение.** *Общее кратное* ок( $a, b, \dots, l$ ) целых  $a, b, \dots, l$  есть всякое целое, которое кратно каждому из  $a, b, \dots, l$ .

**Определение.** *Наименьшее общее кратное* нок( $a, b, \dots, l$ ) или  $[a, b, \dots, l]$  целых  $a, b, \dots, l$  есть наименьшее неотрицательное целое среди всех общих кратных для  $a, b, \dots, l$ .

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

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

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

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

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

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

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

где  $p_1, \dots, p_s$  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  $p_1, \dots, p_s$  есть все простые числа, которые делят хотя бы одно из  $a, b$ . Если простое  $p$  из  $p_1, \dots, p_s$  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.  $a_1 \leq \max(a_1, b_1), \dots, a_s \leq \max(a_s, b_s)$ . Поэтому  $a_1|m, \dots, a_n|m$ .

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

**Замечание.** 1. Если  $a_1 > 1, \dots, a_n > 1$ ,

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

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

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

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

**Теорема.** Пусть  $a \geq 1, b \geq 1$  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  $p_1, \dots, p_s$  есть все различные простые делители чисел  $a$  или  $b$ . Если простое  $p$  из  $p_1, \dots, p_s$  отсутствует в канонической факторизации  $a$ , то добавим к ней множитель  $p^0$ . Аналогично для  $b$ . Далее имеем следующее.

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

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

$$\min(a_1, b_1) + \max(a_1, b_1) = a_1 + b_1,$$

...

$$\min(a_s, b_s) + \max(a_s, b_s) = a_s + b_s, \text{ откуда } dm = ab.$$

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

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

$$2. [a_1, \dots, a_n] = \frac{a_1 \cdot \dots \cdot a_n}{(a_1, \dots, a_n)}.$$

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

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

**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  $a = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}, b = p_1^{b_1} p_2^{b_2} \dots p_s^{b_s}$ , где  $c_i = \min(a_i, b_i) = 0, i = 1, 2, \dots, s$ . Поэтому  $d = (a, b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdot \dots \cdot p_s^{\min(a_s, b_s)} = 1$ .

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

1.  $p \nmid a \leftrightarrow$  в канонической факторизации  $a$  нет множителя  $p$ .
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

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

Получили представление  $c$  в виде непрерывной (цепной) дроби:

$$c = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{q_4 + \dots + \frac{1}{q_{s-1} + \frac{1}{c_s}}}}}$$

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:

$$a = bq_1 + r_2, \frac{a}{b} = q_1 + \frac{r_2}{b} = q_1 + \frac{1}{b/r_2},$$

$$b = r_2q_2 + r_3, \frac{b}{r_2} = q_2 + \frac{1}{r_2/r_3},$$

$$r_2 = r_3q_3 + r_4, \frac{r_2}{r_3} = q_3 + \frac{1}{r_3/r_4},$$

...

$$r_{n-2} = r_{n-1}q_{n-1} + r_n, \frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{1}{r_{n-1}/r_n},$$

$$r_{n-1} = r_nq_n, r_{n+1} = 0, \frac{r_{n-1}}{r_n} = q_n.$$

Тогда непрерывная дробь

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

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

### 1.6.1. Вычисление подходящих дробей

$\delta_s$  можно получить из  $\delta_{s-1}$  заменой  $q_{s-1}$  в  $\delta_{s-1}$  на  $q_{s-1} + 1/q_s$ .

Получим  $P_0 = 1, Q_0 = 0$ . Тогда

$$\delta_1 = \frac{q_1}{1} = \frac{P_1}{Q_1}, \begin{cases} P_1 = q_1, \\ Q_1 = 1, \end{cases} \delta_2 = \delta_1(q_1) \Big|_{q_1 := q_1 + 1/q_2},$$

$$\delta_2 = \frac{q_1 + \frac{1}{q_2}}{1} = \frac{q_1q_2 + 1}{q_2 \cdot 1 + 0} = \frac{q_2P_1 + P_0}{q_2Q_1 + Q_0} = \frac{P_2}{Q_2},$$

$$\delta_3 = \frac{P_1 \left( q_2 + \frac{1}{q_3} \right) + P_0}{Q_1 \left( q_2 + \frac{1}{q_3} \right) + Q_0} = \frac{(P_1q_2 + P_0)q_3 + P_1}{(Q_1q_2 + Q_0)q_3 + Q_1} = \frac{q_3P_2 + P_1}{q_3Q_2 + Q_1} = \frac{P_3}{Q_3},$$

...

$$\delta_s = \frac{q_s P_{s-1} + P_{s-2}}{q_s Q_{s-1} + Q_{s-2}} = \frac{P_s}{Q_s},$$

...

### 1.6.2. Алгоритм вычисления подходящих дробей

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

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

**Пример.** Найдем непрерывную дробь для числа  $105/38$ .

$$105 = 38 \cdot 2 + 29, q_1 = 2,$$

$$38 = 29 \cdot 1 + 9, q_2 = 1,$$

$$29 = 9 \cdot 3 + 2, q_3 = 3,$$

$$9 = 2 \cdot 4 + 1, q_4 = 4,$$

$$2 = 1 \cdot 2, q_5 = 2.$$

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

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  $\delta_s, s > 1$ , 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

$$\begin{aligned} h_s &= (-1)h_{s-1} = (-1)^2 h_{s-2} = (-1)^3 h_{s-3} = \dots = (-1)^{s-1} h_{s-(s-1)} = (-1)^{s-1} h_1 = \\ &= (-1)^{s-1} (P_1 Q_0 - Q_1 P_0) = (-1)^{s-1} (q_1 \cdot 0 - 1 \cdot 1) = (-1)^{s-1} \cdot (-1) = (-1)^s. \end{aligned}$$

Тогда

$$P_s Q_{s-1} - Q_s P_{s-1} = (-1)^s, \quad s > 1, \quad (1.3)$$

$$\delta_s - \delta_{s-1} = (-1)^s / (Q_s Q_{s-1}), \quad s > 1. \quad (1.4)$$

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  $\delta_{s-1}, \delta_s$  и  $|c - \delta_{s-1}| \leq |\delta_s - \delta_{s-1}| \leq 1/(Q_s Q_{s-1})$ .