ВЫСШЕЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАНИЕ

С. Н. ПОЗДНЯКОВ, С. В. РЫБИН

ДИСКРЕТНАЯ МАТЕМАТИКА

Допущено
Министерством образования и науки Российской Федерации
в качестве учебника для студентов высших учебных заведений,
обучающихся по направлениям подготовки «Информатика
и вычислительная техника», «Информационные системы»,
«Информационная безопасность»

ACADEMIA

Москва
Издательский центр «Академия»
2008

УДК 51(075.8)
ББК 22.176я73
П472

Рецензенты:
канд. физ.-мат. наук, доц. *И. В. Артамкин* (Московский государственный институт радиотехники, электроники и автоматики (технический университет));
доц. *М. В. Дмитриева* (Санкт-Петербургский государственный университет, кафедра информатики)

Поздняков С. Н.

П472 Дискретная математика : учебник для студ. вузов / С. Н. Поздняков, С. В. Рыбин. — М. : Издательский центр «Академия», 2008. — 448 с.

ISBN 978-5-7695-3105-7

В учебнике рассмотрены комбинаторика, теория графов, приведены сведения из теории чисел и многочленов, даны общие математические понятия, такие, как отношения, поля, кольца, группы, изложен материал по многочленам нескольких переменных, которые играют большую роль в автоматизации математических вычислений, а также материал по математической логике и теории алгоритмов.

Для студентов высших учебных заведений.

УДК 51(075.8)
ББК 22.176я73

Учебное издание

Поздняков Сергей Николаевич, Рыбин Сергей Витальевич

Дискретная математика

Учебник

Редактор *Л. В. Честная*. Технический редактор *О. Н. Крайнова*.
Компьютерная верстка: *Т. А. Клименко*. Корректоры *В. А. Жилкина*, *Г. Н. Петрова*

Изд. № 101109543. Подписано в печать 31.07.2007. Формат 60 × 90/16.
Бумага тип. № 2. Печать офсетная. Гарнитура «Таймс». Усл. печ. л. 28,0.
Тираж 3000 экз. Заказ №

Издательский центр «Академия». www.academia-moscow.ru
Санитарно-эпидемиологическое заключение № 77.99.02.953.Д.007496.07.04 от 20.07.2004.
117342, Москва, ул. Бутлерова, 17-Б, к. 360. Тел./факс: (495) 334-8337, 330-1092.

Отпечатано в ОАО «Тверской полиграфический комбинат».
170024, г. Тверь, пр-т Ленина, 5. Телефон: (0822) 44-42-15.
Интернет / Home page — www.tverpk.ru. Электронная почта (E-mail) — sales@tverpk.ru

ISBN 978-5-7695-3105-7

ПРЕДИСЛОВИЕ

Курс дискретной математики, читающийся в технических университетах, с первых же лекций открывает интересные перспективы для молодых людей, стремящихся стать специалистами в области информационных технологий.

В чем же особенность этого курса?

❒ Во-первых, дискретная математики строится на базе известных из курса средней школы математических идей. Идеи эти достаточно разноплановы и могут заинтересовать людей с разными интересами и разной математической подготовкой.

❒ Во-вторых, обсуждаемые в курсе дискретной математики идеи быстро приводят к интересным практическим приложениям математической теории. Уже в начале обучения у студентов появляется возможность экспериментировать с ними. Эти эксперименты с прикладными алгоритмами могут реализовываться в курсе информатики и программирования, обычно читающемся параллельно с курсом дискретной математики, либо в индивидуальной работе студентов.

❒ В-третьих, дискретная математика открывает большие перспективы для самостоятельного углубленного изучения курса, что чрезвычайно важно для подготовки мыслящего ученого или инженера.

В настоящее время курс дискретной математики для специальностей, связанных с информатикой, достаточно стабилен. В него входят следующие разделы: комбинаторика, теория графов, теория чисел и многочленов, бинарные отношения, поля, кольца, группы. В то же время положение некоторых разделов, например «Булевы функции», неоднозначно: их включают и в курс дискретной математики, и в курс основ математической логики. Собрав в одном учебнике материалы по дискретному анализу и математической логике, авторы надеются преодолеть это противоречие.

Другой особенностью учебника является более глубокий анализ теории чисел и многочленов. Этот акцент связан с развитием

криптографии, существенно опирающейся на результаты теории чисел.

В книгу также включен материал по многочленам нескольких переменных, которые играют большую роль в автоматизации математических вычислений.

Авторы постарались так скомпоновать учебник, чтобы, с одной стороны, представить материал для практических занятий, познакомить студентов с важными идеями на несложных примерах, которые помогут им освоить в совершенстве необходимую технику вычислений, обсуждаемые алгоритмы, а с другой — последовательно и доказательно изложить теоретический материал, который может быть осмыслен на разных уровнях формализма и необязательно при первом прочтении учебника.

Глава 1

ЦЕЛОЧИСЛЕННЫЕ АЛГОРИТМЫ

1.1. АРИФМЕТИКА ЦЕЛЫХ ЧИСЕЛ

1.1.1. Деление с остатком

Теорема 1.1 (о делимости с остатком). Для любых $a, b \in \in \mathbb{Z}$, где $b \neq 0$, существуют, и притом единственные $q, r \in \mathbb{Z}$, такие, что имеет место представление

$$a = bq + r, \qquad 0 \leqslant r < |b|. \tag{1.1}$$

Доказательство. Не умаляя общности, предположим, что $a > b > 0$. Все остальные случаи или сводятся к этому, или являются тривиальными. Далее будем рассматривать числа, кратные b, т. е. числа вида $b, 2b, 3b, \ldots, kb, \ldots,$. Очевидно, что найдется число $q \geqslant 1$, такое, что

$$bq \leqslant a < (q+1)b. \tag{1.2}$$

Обозначим $r = a - bq$. Из (1.2) следует, что $0 \leqslant r < b$. Представление (1.1) установлено.

Докажем единственность представления (1.1). Пусть

$$a = bq + r = bq_1 + r_1, \qquad 0 \leqslant r < |b|, \qquad 0 \leqslant r_1 < |b|.$$

Тогда $b(q - q_1) = r_1 - r$. Но $|r_1 - r| < |b|$, а $|b(q - q_1)| \geqslant |b|$. Противоречие, таким образом, $q = q_1$, $r = r_1$. ■

Число q в (1.1) называется целой частью дроби $\dfrac{a}{b}$ и обозначается $\left[\dfrac{a}{b}\right]$ или $a \div b$, а число r — остатком и обозначается $\langle a \rangle_b$ или $a \bmod b$.

Определение 1.1. Будем говорить, что a делится на b (и обозначать[1] как $a \vdots b$), если в представлении (1.1) для a, b остаток r равен нулю.

[1] Выражение b делит a часто обозначают, как $b \mid a$.

Историческая справка. Знак $a \vdots b$ для обозначения операции деления числа a на число b впервые ввел Г. Лейбниц в 1684 г.

Сформулируем простейшие свойства делимости, вытекающие непосредственно из определения.

Теорема 1.2. Справедливы следующие утверждения:

1) $a \vdots b, \quad b \vdots c$, тогда $a \vdots c$ (транзитивность деления);

2) $a_1, \ldots, a_k \vdots c$, тогда для любого набора $\lambda_1, \ldots \lambda_k \in \mathbb{Z}$ справедливо $\sum_{i=1}^{k} a_i \lambda_i \vdots c$;

3) $a \vdots b$, тогда $\pm a \vdots \pm b$.

Доказательство. Докажем, для примера, первое свойство. Из условия теоремы имеем: $a = bq$, $b = cl$, тогда $a = (cl)q = c(lq)$. ■

Упражнение 1.1. Докажите самостоятельно свойства 2 и 3 теоремы 1.2.

Замечание 1.1. Последнее свойство позволяет в вопросах делимости ограничиться рассмотрением только натуральных чисел.

1.1.2. Наибольший общий делитель, наименьшее общее кратное и их свойства

Определение 1.2. Пусть $a_1, \ldots, a_k, c \in \mathbb{N}$. Если $c \vdots a_1, \ldots, c \vdots a_k$, то говорят, что c есть *общее кратное* $a_1, \ldots, a_k$. Наименьшее среди всех кратных называют *наименьшим общим кратным* (НОК) и обозначают $M(a_1, \ldots, a_k)$ или $\{a_1, \ldots, a_k\}$. Заметим, что

$$\max\{a_1, a_2, \ldots, a_k\} \leqslant M(a_1, \ldots, a_k) \leqslant a_1 a_2 \cdots a_k.$$

Очевидно, что любое кратное делится на наименьшее общее кратное. Действительно, пусть m — общее кратное $a_1, a_2, \ldots, a_k$. Разделим m на M с остатком. Тогда, согласно (1.1),

$$m = M(a_1, \ldots, a_k)\, q + r, \quad 0 \leqslant r < M(a_1, \ldots, a_k). \tag{1.3}$$

Из (1.3) получаем, что r — также общее кратное $a_1, a_2, \ldots, a_k$, причем меньшее $M(a_1, \ldots, a_k)$. Следовательно, $r = 0$.

Определение 1.3. Пусть $a_1, \ldots, a_k, d \in \mathbb{N}$. Если $a_1 \vdots d, \ldots, a_k \vdots d$, то говорят, что d есть *общий делитель* $a_1, \ldots, a_k$. Наиболь-

ший среди всех делителей называют *наибольшим общим делителем* (НОД) и обозначают $D(a_1, \ldots, a_k)$ или $(a_1, \ldots, a_k)$. Заметим, что

$$1 \leqslant D(a_1, \ldots, a_k) \leqslant \min\{a_1, \ldots, a_k\}.$$

Покажем, что если $d_1, \ldots, d_n$ — общие делители $a_1, \ldots, a_k$, то

$$D(a_1, \ldots, a_k) = M(d_1, \ldots, d_n). \tag{1.4}$$

Действительно, любое a_i по определению является общим кратным чисел $d_1, \ldots, d_n$. Следовательно, $a_i \vdots M(d_1, \ldots, d_n)$, тогда $M(d_1, \ldots, d_n)$ есть общий делитель всех a_i. Но, согласно определению $M(d_1, \ldots, d_n) \vdots d_i$, $i \in\colon n$, отсюда получаем (1.4).

Замечание 1.2. Равенство (1.4) можно использовать в качестве другого определения наибольшего общего делителя.

Введем одно из важнейших понятий теории делимости.

Определение 1.4. Числа $a_1, \ldots, a_k$ называют *взаимно простыми*, если $D(a_1, \ldots, a_k) = 1$.

Установим некоторые свойства наибольшего общего делителя и наименьшего общего кратного.

Теорема 1.3. Справедливы следующие утверждения:

1) $d = D(a_1, \ldots, a_k) \Leftrightarrow D\left(\dfrac{a_1}{d}, \ldots, \dfrac{a_k}{d}\right) = 1$;

2) $d = D(a_1, \ldots, a_k)$, тогда $D(a_1 b, \ldots, a_k b) = db$;

3) если c — общий делитель $a_1, \ldots, a_k$, то $D\left(\dfrac{a_1}{c}, \ldots, \dfrac{a_k}{c}\right) = \dfrac{d}{c}$;

4) $ab = D(a, b)M(a, b)$.

Доказательство. Утверждения 1 — 3 достаточно просты и предлагаются для самостоятельной работы. Докажем утверждение 4. Имеем ab — кратное a и b, поэтому $ab \vdots M(a, b)$. Тогда

$$d := \frac{ab}{M(a, b)}, \qquad \frac{a}{d} = \frac{M(a, b)}{b}, \ \frac{b}{d} = \frac{M(a, b)}{a}. \tag{1.5}$$

Так как $M(a, b)$ делится на a и b, из (1.5) следует, что d — общий делитель a и b. Пусть d_1 — произвольный делитель этих чисел. Тогда

$$\frac{ab}{d_1} = a\left(\frac{b}{d_1}\right) = b\left(\frac{a}{d_1}\right),$$

следовательно, $\dfrac{ab}{d_1}$ — общее кратное a, b, и

$$\frac{ab}{d_1} : M(a,b) = \frac{d}{d_1} \in \mathbb{Z},$$

получаем для произвольного делителя $d \vdots d_1$, таким образом, $d = D(a,b)$. ■

Упражнение 1.2. Докажите самостоятельно утверждения 1 — 3 теоремы 1.3.

Вопрос о нахождении $D(a,b)$ будет решен далее (см. 2.1). Предположим, что имеется эффективный алгоритм его вычисления. Поставим вопрос о вычислении $D(a_1, \ldots, a_k)$. Ответ на этот вопрос дает следующая теорема.

Теорема 1.4. Справедливо равенство

$$D(a_1, a_2, a_3) = D(D(a_1, a_2), a_3)).$$

Доказательство. Введем обозначения: $D(a_1,a_2)=e$, $D(e,a_3)=d$. Тогда в силу транзитивности делимости (теорема 1.2) имеем $a_1, a_2 \vdots d$, но и $a_3 \vdots d$, следовательно, d — общий делитель a_1, a_2, a_3. Пусть d_1 — произвольный общий делитель a_1, a_2, a_3. Тогда $e \vdots d_1$, следовательно, d_1 — общий делитель e, a_3. Тогда $d \vdots d_1$ и, следовательно, $d = D(a_1, a_2, a_3)$. ■

Для наименьшего общего кратного можно получить результат, аналогичный теореме 1.4.

Теорема 1.5. Справедливо равенство

$$M(a_1, a_2, a_3) = M(M(a_1, a_2), a_3)).$$

Установим еще несколько свойств взамно простых чисел.

Теорема 1.6. Если $ab \vdots c$ и $D(a,c) = 1$, тогда $b \vdots c$.

Доказательство. $ab \vdots c$ и $ab \vdots a$, следовательно, ab — кратное чисел a и c. Тогда $ab \vdots M(a,c)$, но, согласно теореме 1.3, $M(a,c) = ac$. Следовательно, $ab \vdots ac$. Отсюда получаем требуемое. ■

Упражнение 1.3. Докажите утверждение: если $D(a,c) = 1$, то $D(ab,c) = D(b,c)$.

1.1.3. Простые числа

Определение 1.5. Натуральное число $p > 1$ называют *простым*, если оно делится только на $\pm p$ и на ± 1.

Теорема 1.7. Пусть p — простое число. Справедливо утверждение: $ab \vdots p$ тогда и только тогда, когда $a \vdots p$ или $b \vdots p$.

Доказательство. Пусть $ab \vdots p$. Предположим, что a не делится на p. Тогда $D(a, p) = 1$. По теореме 1.6 получаем требуемое. В обратную сторону утверждение теоремы очевидно. ■

Лемма 1.1. Любое $a \in \mathbb{Z}, a \neq 1$ имеет по крайней мере один простой делитель.

Доказательство. Пусть $d_1, d_2, \ldots, d_n$ — все положительные делители числа a, кроме 1. Положим $p = \min\{d_1, d_2, \ldots, d_n\}$. Если бы p было составным, то его делитель (меньший, чем само p) был бы делителем a. Противоречие с определением p. ■

Теорема 1.8 (основная теорема теории делимости). Любое число $a \in \mathbb{Z}$ раскладывается и только одним способом на простые сомножители. Соединив одинаковые множители в степени, получаем ***каноническое разложение***

$$a = p^{\alpha} q^{\beta} r^{\gamma} \cdots, \text{ где } p, q, r - \text{ простые числа; } \alpha, \beta, \gamma \geqslant 1. \qquad (1.6)$$

Доказательство. По лемме 1.1 любое число a имеет простой делитель p. Представим его в виде pa_1. Если a_1 — составное число, то воспользуемся леммой 1.1 для a_1. Заметим, что $a_1 < a$, поэтому на некотором шаге получим a_k простое число. Таким образом, имеем представление

$$a = p_1 p_2 p_3 \cdots p_k, \text{ где } p_1, p_2, p_3 \cdots p_k \text{ — простые числа.}$$

Объединив одинаковые множители в степени, приходим к (1.6). Докажем единственность представления (1.6). Пусть имеется два различных представления:

$$a = p_1 p_2 p_3 \cdots p_k = q_1 q_2 q_3 \cdots q_n. \qquad (1.7)$$

Тогда $p_1 p_2 p_3 \cdots p_k \vdots q_1$. По теореме 1.7 один из сомножителей слева делится на q_1. Пусть, для определенности, $p_1 \vdots q_1$. Но p_1 и q_1 — простые числа. Поэтому $p_1 = q_1$. Тогда (1.7) можно переписать в виде

$$p_2 p_3 \cdots p_k = q_2 q_3 \cdots q_n.$$

Повторив эту процедуру, приходим к единственности представления (1.6). ■

Следствие 1.1. Пусть a и b представлены в каноническом виде (1.6):

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}, \quad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}.$$

Тогда

$$D(a,b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_n^{\gamma_n}, \quad M(a,b) = p_1^{\delta_1} p_2^{\delta_2} \cdots p_n^{\delta_n},$$

где $\gamma_i = \min\{\alpha_i, \beta_i\}$, а $\delta_i = \max\{\alpha_i, \beta_i\}$.

Историческая справка. В 1876 г. французский математик Ф. Люка доказал, что число $2^{127} - 1$ является простым, и 75 лет оно оставалось наибольшим из известных простых чисел, что не покажется удивительным, если на него взглянуть:

$$2^{127} - 1 = 170\,141\,183\,460\,469\,231\,731\,687\,303\,715\,884\,105\,727.$$

В настоящее время составлены таблицы всех простых чисел, не превосходящих 50 миллионов, далее известны только отдельные их представители. Укажем здесь два самых больших из известных на сегодняшний момент простых числа: $2^{44497} - 1$ и $2^{86243} - 1$. Последнее число записано пока в книгу рекордов Гиннесса, в нем 25 962 десятичных знака.

1.1.4. Решето Эратосфена. Разложение числа на простые множители

В связи с полученным представлением (1.6) возникает необходимость построить эффективные алгоритмы для решения следующих задач:

1) найти все простые числа в данном интервале;

2) для произвольного числа $a \in \mathbb{Z}$ получить его разложение в виде (1.6).

Для решения первой задачи рассмотрим алгоритм, носящий название *решето Эратосфена*. Он позволяет найти все простые числа, не превосходящие N.

Алгоритм 1.1 (решето Эратосфена).

Шаг 1. Вычеркиваем все числа, кратные 2 (каждое второе, кроме 2). Полагаем $p_1 = 2, k = 1$.

Шаг k+1. Полагаем $k = k + 1$ и p_k — первое невычеркнутое число после p_{k-1}. Вычеркиваем все числа, стоящие на местах, кратных p_k, кроме него самого. Повторяем этот шаг, пока $p_k < N$.

Замечание 1.3. Достаточно работать только с нечетными числами, при этом $p_1 = 3$. Алгоритм заканчивает работу, как только выполнено условие $p_k \geqslant \sqrt{N}$, все числа, остающиеся невычеркнутыми, — до самого N, будут простыми. Это вытекает из следующей теоремы.

Теорема 1.9. Всякое составное число a имеет делитель $b \leqslant \leqslant \sqrt{a}$.

Доказательство. Если $a = bc$, то из пары чисел b, c одно больше $\sqrt{a}$, а другое меньше, за исключением случая, когда a — точный квадрат, тогда $b = c = \sqrt{a}$. ■

***Пример 1.1* (*решето Эратосфена*).** Пусть $N = 50$. Тогда после работы алгоритма получаем следующую картину (на месте вычеркнутых чисел стоит знак $*$):

$$2\ 3\ 5\ 7\ 9\ 11\ 13\ *\ 17\ 19\ *\ 23\ *\ *\ 29\ 31\ *\ *\ 37\ *\ 41\ 43\ *\ 47\ 49.$$

Возникает вопрос: сколько же простых чисел? Ответ был получен еще Евклидом.

Теорема 1.10 (теорема Евклида). Множество простых чисел бесконечно.

Доказательство. Допустим конечность множества простых чисел: $\{p_1, p_2, p_3, \ldots, p_k\}$. Положим $p = p_1 p_2 p_3 \cdots p_k + 1$. Очевидно, что число p не делится ни на одно из p_i. Таким образом, либо p — простое, либо имеет простой делитель, больший любого из p_i. Полученное противоречие и доказывает теорему. ■

Перейдем к решению второй поставленной задачи: разложению числа a на простые сомножители в виде (1.6). Начнем с простейшего алгоритма, носящего название *метод пробных делителей.*

Алгоритм 1.2 (метод пробных делителей). Используем последовательность *пробных делителей* — простых чисел:

$$2 = p_0 < p_1 < p_2 < \cdots < p_k \leqslant \sqrt{a}.$$

Введем следующие обозначения:

- $k = 0, 1, 2, \ldots$ — номер текущего делителя p_k (из пробной последовательности);

• $i = 0, 1, 2, \ldots$ — номера найденных делителей числа a (будем обозначать их d_i).

Шаг 1. $k := 0, i := 0$.

Шаг 2 (проверка окончания). Если $a = 1$, то алгоритм заканчивает работу. Найденные делители находятся в массиве d_i.

Шаг 3. $a := p_k q + r$.

Шаг 4. Если $r \neq 0$ (т. е. a не делится на p_k), то переходим на *шаг 6.*

Шаг 5 (a делится на p_k). Полагаем $d_i := p_k, i := i + 1, a := q$. Возвращаемся на *шаг 2.*

Шаг 6. Если $q > p_k$, то полагаем $k := k + 1$ и переходим на *шаг 3.*

Шаг 7. a — простое число. Полагаем $d_i := a$. Алгоритм заканчивает работу.

Пример 1.2 (метод «пробных делителей»). Пусть $a = 6\,930$. Возьмем последовательность пробных делителей

$$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots, \}$$

1) $a = 2 \cdot 3\,465, d_0 = 2, i = 1, a = 3\,465$;
2) $a = 2 \cdot 1\,732 + 1, k = 1$;
3) $a = 3 \cdot 1\,155, d_1 = 3, i = 2, a = 1\,155$;
4) $a = 3 \cdot 385, d_2 = 3, i = 3, a = 385$;
5) $a = 3 \cdot 128 + 1, k = 2$;
6) $a = 5 \cdot 77, d_3 = 5, i = 4, a = 77$;
7) $a = 5 \cdot 15 + 2, k = 3$;
8) $a = 7 \cdot 11, d_4 = 7, i = 5, a = 11$;
9) $a = 7 \cdot 1 + 4, d_5 = 11$.

Имеем: $a = 6\,930 = 2 \cdot 3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$.

Легко видеть, что описанный алгоритм эффективно работает на небольших числах. При их увеличении быстро растет число «холостых» делений. Рассмотрим алгоритм, который, *используя только операции умножения и сложения (без делений)*, позволяет представить любое число в виде произведения двух (не обязательно простых) сомножителей.

Алгоритм 1.3 (метод Ферма). Не умаляя общности, можно считать, что исходное число a является нечетным[1]. Выделить степени двойки достаточно легко (сдвигами вправо двоичного представления числа). Будем искать представление a в виде

[1]Метод не работает для четных чисел, содержащих в разложении 2 в первой степени. Например, $26 = 2 \cdot 13$ или $50 = 2 \cdot 5^2$.

Итерация	$R(x,y)$	R_x	R_y	Итерация	$R(x,y)$	R_x	R_y
0	-25	29	1	2	3	31	3
1	4	31	1	3	0	31	5

$$a = x^2 - y^2 = (x-y)(x+y).$$

Введем обозначения: $R(x,y) = (x-y)(x+y) - a$.

Требуется, поочередно увеличивая x и y на 1, добиться равенства $R(x,y) = 0$. Заметим, что

$$R(x+1,y) = (x-y+1)(x+y+1) - a = R(x,y) + 2x + 1,$$

$$R(x,y+1) = (x-y-1)(x+y+1) - a = R(x,y) - (2y+1).$$

Чтобы лишний раз не умножать на 2, введем обозначения: $R_x = 2x+1$, $R_y = 2y+1$. Заметим, что при увеличении x или y на 1 R_x или R_y увеличиваются соответственно на 2. Для простоты изложения считаем, что известна приблизительная оценка целой части $\sqrt{a}$ — обозначим ее через $\bar{a}$.

Шаг 1 (инициализация). $R_x := 2\bar{a}+1$, $R_y := 1$, $R(x,y) := \bar{a}^2 - a$.

Шаг 2. Если $R(x,y) \leqslant 0$, то переходим на *шаг 4*.

Шаг 3. $R(x,y) := R(x,y) - R_y$, $R_y := R_y + 2$. Возвращаемся на *шаг 2*.

Шаг 4 (проверка окончания). Если $R(x,y) = 0$, то алгоритм заканчивает работу. При этом

$$a = \frac{R_x - R_y}{2}\left(\frac{R_x + R_y}{2} - 1\right).$$

Шаг 5. $R(x,y) = R(x,y) + R_x$, $R_x = R_x + 2$. Возвращаемся на *шаг 2*.

Пример 1.3 (метод Ферма). Пусть $a = 221$, тогда $\bar{a} = 14$. Протокол[1] работы алгоритма представлен в табл. 1.1.

Имеем $a = 221 = 17 \cdot 13$.

Комбинируя *методы Ферма и пробных делителей*, можно построить эффективный алгоритм для разложения достаточно большого числа a на простые сомножители в виде (1.6).

[1]Поля, изменяющиеся на данной итерации, выделены серым цветом.

1.1.5. Позиционная запись натуральных чисел

Определение 1.6. Упорядоченный набор неотрицательных целых чисел $(a_n a_{n-1} \dots a_1 a_0)_p$ называют p-ичной записью натурального числа c (представлением числа c в p-ичной системе счисления или просто p-ичным числом), если

$$c = p^n a_n + p^{n-1} a_{n-1} + \dots + p a_1 + a_0, \tag{1.8}$$

где p — натуральное число, большее 1, $0 \leqslant a_k < p$ и $a_n \neq 0$.

Замечание 1.4. Числа a_k в p-ичной записи называют цифрами и обычно обозначают отдельными символами, например $10 = A$, $11 = B$ и т. д.

Теорема 1.11. Каждое натуральное число имеет единственную p-ичную запись.

Доказательство. Пусть c имеет две различные p-ичные записи: $a_n a_{n-1} \dots a_1 a_0$ и $b_m b_{m-1} \dots b_1 b_0$. Тогда

$$\begin{aligned} c = p^n a_n + \dots + p a_1 + a_0 = p\left(p^{n-1} a_n + \dots + a_1\right) + a_0 = \\ = p c_1 + a_0 c = p^m b_m + \dots + p b_1 + b_0 = \\ = p\left(p^{m-1} b_m + \dots + b_1\right) + b_0 = p c_2 + b_0. \end{aligned}$$

Так как частное и остаток при делении на p определяются однозначно,

$$a_0 = b_0 \text{ и } c_1 = p^{n-1} a_n + \dots + a_1 = p^{m-1} b_m + \dots + b_1 = c_2.$$

Применив аналогичные рассуждения к c_1 и c_2, получим $a_1 = b_1$ и т. д. ■

Замечание 1.5. Существуют и другие способы позиционной записи натуральных чисел, т. е. представление их упорядоченными наборами цифр.

Пример 1.4 (факториальная запись).

$$c = (a_n a_{n-1} \cdots a_1)_! \Leftrightarrow c = a_n n! + a_{n-1}(n-1)! + \dots + a_1 \cdot 1!,$$

где $0 \leqslant a_k \leqslant k$, $a_n \neq 0$.

Упражнение 1.4. Докажите единственность факториальной записи натуральных чисел.

Замечание 1.6. Алгоритм построения факториальной записи числа будет получен далее (см. подразд. 1.6.8, алгоритм 1.34).

1.1.6. Алгоритмы арифметических действий с p-ичными записями натуральных чисел

Алгоритмы сложения, вычитания, умножения «столбиком» и деления «уголком» для p-ичных записей чисел совпадают с известными алгоритмами для десятичных записей, если заменить таблицы сложения (вычитания) и умножения (деления). В этом случае говорят о выполнении операций в p-ичной арифметике.

Алгоритм 1.4. Производит сложение p-ичных чисел $a = (a_n \cdots a_0)_p$ и $b = (b_m \cdots b_0)_p$. Результат — число $c = (c_k \cdots c_0)_p$.

ЕСЛИ $n < m$ ТО
  $a \leftrightarrow b$; $n \leftrightarrow m$; (тем самым длина числа a станет не меньше длины b)
КЕ
  $i := 0$; $s := 0$; (i — номер разряда, s — величина переноса в старший разряд)
ЦИКЛ-ПОКА $i \leqslant m$
  $c_i := (a_i + b_i + s) \bmod p$; (вычисление очередной с конца цифры результата)
  $s := (a_i + b_i + s) \div p$; (вычисление величины межразрядного переноса)
  $i := i + 1$ (переход к следующему разряду)
КЦ
ЦИКЛ-ПОКА $i \leqslant n$ (продолжение сложения числа после «прохождения» старшего разряда числа меньшей длины)
  $c_i := (a_i + s) \bmod p$;
  $s := (a_i + s) \div p$;
  $i := i + 1$
КЦ
ЕСЛИ $s > 0$ ТО (формирование старшего разряда результата, если длина результата больше длины слагаемых)
  $c_{n+1} := s$
КЕ

Алгоритм 1.5. Производит умножение числа $a = (a_n \cdots a_0)_p$ на цифру $b = (b_0)_p$. Результат $ab = c = (c_m \cdots c_0)_p$.

$s := 0$
ЦИКЛ ПО i ОТ 0 ДО n
  $c_i := (a_i b_i + s) \bmod p$; $s := (a_i b_i + s) \div p$
КЦ;
ЕСЛИ $s > 0$, ТО $m := n + 1$; $c_m := s$ ИНАЧЕ $m := n$

Алгоритм 1.6. Производит умножение числа $a = (a_n ... a_0)_p$ на число p^k (сдвиг на k разрядов). Результат $ap^k = c = (c_m \cdots c_0)_p$.

Таблица 1.2

а

$(+)_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	10
2	2	3	4	10	11
3	3	4	10	11	12
4	4	10	11	12	13

б

$(\times)_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	11	13
3	0	3	11	14	22
4	0	4	13	22	31

$m := n + k$;
ЦИКЛ ПО i ОТ n ДО 0 $\quad c_{i+k} := a_k \quad$ КЦ
ЦИКЛ ПО i ОТ $k-1$ ДО 0 $\quad c_i := 0; \quad$ КЦ

Алгоритм 1.7. Производит перемножение p-ичных чисел $a = (a_n \dots a_0)_p$ и $b = (b_k \dots b_0)_p$. Результат $ab = c = (c_m \dots c_0)_p$.

$c := 0$;
ЦИКЛ ПО i ОТ 0 ДО k
$\quad c := c + (ab_i)p^i$; (поразрядное умножение со сдвигом
КЦ выполняется по алгоритмам 1.5 и 1.6)

Задание 1.1. Упростите алгоритмы арифметических операций для двоичных чисел.

Задание 1.2. Сформулируйте алгоритмы сложения и умножения натуральных чисел в факториальной записи.

Задание 1.3. Напишите алгоритмы вычитания и деления нацело, основываясь на таблицах вычитания и деления p-ичных чисел.

Пример 1.5. Используя рассмотренные алгоритмы 1.4—1.7, построим таблицы сложения (табл. 1.2, *а*) и умножения (табл. 1.2, *б*) для 5-ичных чисел.

1.1.7. Алгоритмы перевода p-ичной записи натурального числа в q-ичную

Первый из алгоритмов перевода использует p-ичную арифметику, второй — q-ичную. В основе первого алгоритма лежит та же идея, что и в доказательстве единственности p-ичной записи натурального числа.

Алгоритм 1.8. Переводит число из p-ичной записи вида $(a_n \dots a_0)_p$ в q-ичную $(b_m \dots b_0)_q$ в p-ичной арифметике.

$i := 0$;
ЦИКЛ-ПОКА $a \neq 0$
$b_i := a \bmod q$; (деление a на q выполняется в p-ичной
$a := a \div q$ арифметике)
$i := i + 1$
КЦ
$m := i - 1$

Второй алгоритм основан на так называемой схеме Горнера (см. (1.61)):

$$a = (a_n a_{n-1} \cdots a_0)_p = a_n p^n + a_{n-1} p^{n-1} + \cdots + a_1 p + a_0 = \\ = ((...((a_n p + a_{n-1})p + a_{n-2})p + \cdots + a_1)p + a_0). \qquad (1.9)$$

Алгоритм 1.9. Производит перевод чисел из p-ичной $(a_n \cdots a_0)_p$ записи в q-ичную $(b_m \cdots b_0)_q$ в q-ичной арифметике.

$b := 0$;
ЦИКЛ ПО i ОТ n ДО 0
$b := bp + a_i$; (действия выполняются в q-ичной
КЦ арифметике)

Замечание 1.7. При $p > q$ применение последнего алгоритма подразумевает предварительный перевод всех цифр в q-ичную запись. Аналогично, при $p < q$ алгоритм 1 подразумевает дополнительные действия по переводу цифр порождаемой записи из p-ичной записи в q-ичную.

1.1.8. Алгоритм эффективного возведения числа в натуральную степень

Схема Горнера (1.9) может быть применена для построения эффективного алгоритма возведения числа a в натуральную степень m. Рассмотрим двоичную запись числа m:

$$m = (b_n \dots b_0)_2 = 2^n b_n + \cdots + 2b_1 + b_0.$$

Тогда

$$a^m = a^{2m_1 + b_0} = (a^{m_1})^2 a^{b_0} = \begin{cases} (a^{m_1})^2 & \text{при } b_0 = 0, \\ (a^{m_1})^2 a & \text{при } b_0 = 1, \end{cases}$$

$$\text{где} \quad m_1 = (b_n \dots b_1)_2 = 2^n b_n + \cdots + 2b_2 + b_1.$$

Алгоритм 1.10. Возводит число a в степень $m = (b_n \dots b_0)_2$. Результат $c = a^m$.

$c := 1$;
ЦИКЛ ПО i ОТ n ДО 0
ЕСЛИ $b_i = 0$ ТО $c := c^2$ ИНАЧЕ $c := c^2 a$ КЕ
КЦ

Таблица 1.3

Значение i	Значение c
6	$c = c^2 \cdot 27(391) = 27$
5	$c = c^2 \cdot 27 = 27^3(391) = 19\,683(391) = 133$
4	$c = c^2 \cdot 27 = 133^2 \cdot 27(391) = 477\,603(391) = 192$
3	$c = c^2 \cdot 27 = 192^2 \cdot 27(391) = 995\,328(391) = 233$
2	$c = c^2 \cdot 27 = 233^2 \cdot 27(391) = 1\,465\,803(391) = 335$
1	$c = c^2 = 335^2(391) = 112\,225(391) = 8$
0	$c = c^2 \cdot 27 = 8^2 \cdot 27(391) = 1\,728(391) = 164$

Замечание 1.8. Предложенный алгоритм легко модифицируется для возведения a в степень m в кольце $\mathbb{Z}_k$. Для этого достаточно операцию умножения осуществлять в кольце вычетов по модулю k (см. теорему 1.23).

Пример 1.6. Вычислим $27^{125}(391)$. Согласно алгоритму 1.10 имеем (табл. 1.3):

$$m = 125 = (1111101)_2,\ a = 27,\ c = 1,\ i = 6, 5, \ldots, 0.$$

Таким образом, $27^{125}(391) = 164$.

Задание 1.4. Сколько операций умножения (возведение в квадрат — это тоже операция умножения) выполнит алгоритм при вычислении: а) a^{2^k}; б) $a^{2^{k-1}}$?

Задание 1.5. Докажите, что количество умножений в алгоритме возведения числа в степень m не превышает $2\lfloor \log_2 m \rfloor$.

Задание 1.6. Найдите формулу, выражающую число умножений в алгоритме возведения a в степень m через l — число цифр в двоичной записи m и r — число нулей в двоичной записи m.

1.2. АЛГОРИТМ ЕВКЛИДА И ЦЕПНЫЕ ДРОБИ

1.2.1. Классический алгоритм Евклида

Историческая справка. О жизни Евклида не имеется никаких достоверных сведений. Предположительно считается, что он жил во времена Птолемея I (IV — III вв. до н. э.). Наиболее знаменитое и выдающееся произведение Евклида — тринадцать книг его «Начал». Это