Для того, чтобы не усложнять работу с текущими значениями параметров, момент, когда нужна работа с этими значениями, откладывается до выполнения трех арифметических операций. Это делается при помощи формулы ► **is** <> ◄, фигурирующей в настраиваемой части функции. Точная семантика этого обозначения следующая. Если он не оснащен одним из параметров подпрограммы, имеющим значение по умолчанию, то компилятор использует в подпрограмме то же имя, что и настраиваемый параметр, и то же значение параметра. Таким образом, программа, использующая эту функцию, чтобы найти НОД, может быть реализована следующим образом:

function *Ring_GCD* **is new** *GCD (integer, 0)*,

где передаваемый параметр для действий целого типа и константа 0.

Перейдем к реализации функции *GCD* (т.е. НОД). Для упрощения работы с элементами поля, для того, чтобы сделать эту работу более похожей на исходный алгоритм, определяется тип *Pair*. Надо отметить, что единственное, в чем нуждается функция*GCD*, это оператор **mod**. На практике, в общем случае, все что нужно, — это, прежде всего, оператор деления. Поэтому оператор деления, снабженный настраиваемым параметром, находит функцию остатка, используемую в алгоритме для вычисления НОД, сравнительно просто.

3.4. Сравнение эффективности различных делений

Разумеется, функция, о которой говорилось в предыдущем разделе, достаточна для вычисления НОД двух элементов евклидова кольца. Но нас интересует также эффективность предложенных методов, а для такой оценки одних этих функций недостаточно. Действительно, чтобы сравнить эти методы, можно написать программу вычисления НОД двух целых чисел, параметризовав ее используемым оператором деления (или нахождения остатка). Если эта программа позволит отследить все промежуточные результаты, то можно наблюдать сходимость метода и сделать некоторые предположения в отношении сложности.

Мы не будем заниматься здесь подробно этой функцией (ее выполнение очень просто). Ограничимся приведением нескольких результатов, иллюстрирующих полученную разницу в сложности и в результатах, когда используются различные операторы нахождения остатка. Функции, которые используются (в порядке следования), деление, отвечающее оператору **rem** в языке Ада, деление с использованием оператора **mod** и, наконец, центрированное деление (которое отвечает стандартному оператору, заложенному в большинстве языков программирования, но который легко может привести к неверному результату).

Сложность вычисления НОД сильно отличается в зависимости от используемой функции, как показывает таблица 1.

i	Остаток **rem** в яз. Ада	Остаток **mod** в яз. Ада	**Центриров. остаток**
1	$204 = -126 \times -1 + 78$	$204 = -126 \times -2 + -48$	$204 = -126 \times -2 + -48$
2	$-126 = 78 \times -1 + -48$	$-126 = -48 \times 2 + -30$	$-126 \times 3 + 18$
3	$78 = -48 \times -1 + 30$	$-48 = -30 \times 1 + -18$	$-48 = 18 \times -3 + 6$
4	$-48 = 30 \times -1 + -18$	$-30 = -18 \times 1 + -12$	$18 = 6 \times 3 + 0$
5	$30 = -18 \times -1 + 12$	$-18 = -12 \times 1 + -6$	
6	$-18 = 12 \times -1 + -6$	$-12 = -6 \times 2 + 0$	
7	$12 = -6 \times -2 + 0$		

Таблица 1: Последовательность частных для различных евклидовых делений

Центрированное деление дает в действительности наименьшее количество итераций, результат, на котором мы остановимся в разделе 6. Однако точка зрения, заключающаяся в том, что НОД надо вычислять в $\mathbb{Z}$, используя наименьший остаток, уязвима. Она не учитывает того факта, что оператор центрированного деления реализуется за большее время из-за логики программирования, тогда как два других вообще свободны от этого недостатка и могут быть прямо реализованы в железе. То, что выигрывается в теории алгоритмов, теряется при программировании на машине. Ах, информатика без машин! На этом примере можно также увидеть неединственность НОД. Два простых алгоритма дают значение —6, в то время как третий дает значение 6.

3.5. Факториальность евклидовых колец без делителей нуля

Следующая лемма рассматривает поведение алгоритма Евклида φ по отношению к включению идеалов и показывает, что евклидово кольцо нётерово.

***Лемма* 1**
Пусть φ — евклидов алгоритм кольца A.

(i) Неравенство $\varphi(0) < \varphi(b)$ верно для любого $b \in A^*$.

(ii) Отображение $\tilde{\varphi}$ (со значениями в области значений φ), определенное на множестве ненулевых идеалов A соотношением $\tilde{\varphi}(1) = min\{\varphi(a) \mid a \in I \backslash 0\}$ — строго убывающее отображение множества ненулевых идеалов из A во вполне упорядоченное множество. Значит, A нётерово.

Доказательство.

(*i*) Пусть $b \in A^*$. Алгоритм Евклида 27, применяемый к $a \neq 0$ и b, дает последовательность $(r_i)_{0 \leqslant i \leqslant n+1}$ с $\varphi(r_{n+1}) < \varphi(r_n) < \cdots < \varphi(r_2) < \varphi(r_1)$, где $r_{n+1} = 0$ и $r_1 = b$. Следовательно, $\varphi(0) < \varphi(b)$ для любого $b \in A^*$.
(*ii*) Пусть теперь I и J два ненулевых идеала, для которых $I \supsetneq J$. Пусть $a \in I \backslash \{0\}$ такой, что $\varphi(a) = \tilde{\varphi}(I)$. Идеал Aa, содержащийся в I, строго содержится в J. Выберем $x \in J \backslash Aa$ и осуществим евклидово деление x на a: $x = ag + r$, где $\varphi(r) < \varphi(a)$. Так как $x \notin Aa$, то r — ненулевой элемент из J. Отсюда $\tilde{\varphi}(J) \leq \varphi(r) < \varphi(a) = \tilde{\varphi}(I)$ что заканчивает доказательство леммы.

■

***Предложение* 2**
Всякое евклидово кольцо без делителей нуля является факториальным, нётеровым и кольцом Безу.

Доказательство.

Предыдущая лемма показывает, что всякое евклидово кольцо (без делителей нуля или с ними) нётерово. Согласно предложению 9, всякий элемент из $A^* \backslash U(A)$ является произведением неприводимых элементов. С учетом того, что — кольцо Безу, предложение доказано.

■

Итак, мы доказали, в частности, что всякий идеал евклидова кольца имеет конечный тип. Следующее предложение еще интереснее.

***Предложение* 3**
Всякий ненулевой идеал евклидова кольца A главный.

Доказательство.

Вот прямое и классическое доказательство этого факта. Пусть I — ненулевой идеал в A и $a \in I \backslash \{0\}$ такой элемент, что $\varphi(a) = \min\{\varphi(x) | x \in I \backslash 0\}$ (такое определение имеет смысл, так как значения φ принадлежат вполне упорядоченному множеству). Элемент порождает I. В самом деле, для $x \in I$ осуществим евклидово деление x на a: $x = aq + r$, где $\varphi(r) < \varphi(a)$. Принадлежность r к I и минимальность $\varphi(a)$ дают $r = 0$. Следовательно, $x = aq$, что и требовалось доказать.
Внимательный читатель обратит внимание на аналогию с доказательством леммы 29. Действительно, если I — ненулевой идеал и $\in I \backslash \{0\}$ такой, что $\varphi(a) = \tilde{\varphi}(I)$, то $Aa \subset I$ и $\tilde{\varphi}(Aa) = \tilde{\varphi}(I)$, ввиду строгого убывания $\tilde{\varphi}$. Значит, $Aa = I$.

Наконец, имеется третий довод! Так как кольцо A конечного типа (A нётерово), то его идеал конечного типа и потому главный (A является кольцом Безу)...

■

Замечание. Можно заметить, что в $\mathbb{Z}$ или в $K[X]$ имеется эффективный метод (раздел 6) вычисления НОД. Однако проблема разложения целых чисел на простые множители (или многочлена в произведение неприводимых) более трудна для решения. Есть, впрочем, проблема, имеющая, по-видимому, промежуточную сложность. Это задача проверки на простоту целого числа (или неприводимость многочлена). Читатель - скептик приглашается для проверки неприводимости для случая факторизации, с одной стороны, числа, имеющего в своей записи 78 десятичных цифр:

$$2^{257} - 1 = 231\,584\,178\,474\,632\,390\,847\,141\,970\,017\,375\,815$$
$$706\,539\,969\,331\,281\,128\,078\,915\,168\,015\,826\,259\,279\,871,$$

а с другой — полинома с коэффициентами из $\mathbb{Z}\backslash 2\mathbb{Z} : X^{2^{30}} — X$.

4. Многочлены с коэффициентами из поля

Читатель, несомненно, знаком с некоторыми результатами относительно распределения простых чисел или с теоремой Евклида, утверждающей бесконечность множества простых чисел. Что известно для многочленов? На самом деле, применение аргумента Евклида показывает, что существует бесконечное множество унитарных неприводимых многочленов над всяким полем. Для некоторых полей можно доказать существование неприводимых многочленов любой заданной степени. Например, над полем $\mathbb{Q}$ рациональных чисел многочлен $X^n — 2$ является неприводимым для любого натурального числа n (что совершенно неочевидно и требует доказательства, например, для $n = 2$ это равносильно иррациональности $\sqrt{2}$).

Мы докажем, что для всякого простого p и для любого натурального числа n существует неприводимый многочлен степени n по модулю p, без явного указания его, — результат, который можно рассматривать как замечательный. Мы найдем также формулу, позволяющую подсчитать количество таких многочленов, исходя из которой читатель сможет найти плотность множества неприводимых многочленов по модулю p, имеющих данную степень. Но прежде всего, представим в явном виде алгоритм Евклида деления многочленов.

4.1. Евклидово деление в $K[X]$ (K - поле)

***Теорема* 4** (евклидово деление многочленов)

Пусть A и B два многочлена с коэффициентами в поле K, B — ненулевой. Существует алгоритм, позволяющий вычислить такие многочлены Q и R, что $= BQ + R$*и* $deg(R) < deg(B)$*. Более того, указанная пара (P, Q) многочленов определяется единственным образом.*

Дидактический пример

Рассмотрим сначала пример, который позволит лучше понять доказательство теоремы. Осуществим евклидово деление в $\mathbb{Q}[X]$ многочлена $A = 2X^5 - X^4 + 6X^3 - 9X^2 + 7X + 2$ на многочлен $B = 2X^2 - X + 1$ (на самом деле деление производится в $\mathbb{Z}[X]$, но это несущественно).

Разделим $2X^5$ на $2X^2$, старшие одночлены в A и B соответственно. Получим $1{\times}X^3$ (старший одночлен частного). Теперь можно вычислить A—$B{\times}1{\times}X^3$ и получить многочлен степени ≤ 4. Наконец, заменим B на A—$B \times 1 \times X^3$ и повторим для A и B описанную выше операцию... Оформим действия в виде следующей таблицы, форма которой читателю, возможно, знакома:

$$\begin{array}{rrrrrr|l} 2X^5 & -3X^4 & +6X^3 & -9X^2 & +7X & +2 & 2X^2 - X + 1 \\ \cline{7-7} 0 & -2X^4 & +5X^3 & & & & X^3 - X^2 + 2X - 3 \\ & 0 & +4x^3 & -8X^2 & & & \\ & & 0 & -6X^2 & +5X & & \\ & & & 0 & +2X & +5 & \end{array}$$

Частное есть многочлен $Q = X^3$—$X^2 + 2X$—3, в то время как остаток $R = 2X + 5$.

Рассуждения, встретившиеся в описанном выше примере, должны быть формализованы не только ради математической деонтологии, но, главным образом, для того, чтобы показать рекуррентную основу, поддающуюся переделке в алгоритм, а затем в программу. Очевидно, что читатель легко сможет проследить на предыдущем примере доказательство теоремы, которое приводится ниже.

Доказательство теоремы 32

Пусть $n = deg(A)$, $m = deg(B)$ и b_m — старший коэффициент полинома B. Определим рекуррентным образом многочлены R_{m+k} для $k = n$—m, n—m—1, $..., 1, 0,$—1. На шаге к предположим, что верно равенство

$$A = B \times (...) + R_{m+k}, \text{ где } \deg(R_{m+k}) \leq m + k,$$

a (...) — многочлен, название которого несущественно. Начнем рекурсию, положив $k = n—m$ и положив $R_n = A$ (получим $A = B \times 0 + A$). Если r_{m+k} обозначает коэффициент при X^{m+k} многочлена R_{m+k} и $q_k = r_{m+k}/b_m$, то запишем $A = B \times (... + q_k X^k) + (R_{m+k} - Bq_k X^k)$. Достаточно определить R_{m+k-1} с помощью равенства $R_{m+k-1} = R_{m+k}—Bq_k X^K$ и проверить, многочлен ли это степени $\leq m + K—1$. Получаем следующую рекуррентную схему:

$$R_n = A \text{ и } q_k = r_{k+m}/b_m,\ R_{m+k-1} = R_m + k - Bq_k X^k,\ k = n - m, ..., 1, 0,$$

в которой выполняется порождающее равенство $(0 \leq k \leq n—m + 1)$:

$$A = B\left(\sum_{j-k}^{n-m} q_j X^j\right) + R_{k+m-1} \text{ и } \deg(R_{k+m-1}) \leq k + m - 1,$$

дающее для $k := 0 : A = B\sum_{j=0}^{n-m} q_j X^j + R_{m-1}$ с $\deg(R_{m-1}) \leq m - 1 < \deg(B)$, что заканчивает описание полученного алгоритма евклидова деления. Доказательство единственности евклидова деления очень просто и предоставляется читателю.

***Следствие* 5**

Кольцо K[X] многочленов с коэффициентами в поле K является евклидовым кольцом без делителей нуля, евклидовым относительно степени (со значением в множестве $\{\infty\} \cup \mathbb{N}$).

Алгоритм 2, отвечающий полученной рекуррентной схеме доказательства теоремы 32, существенно использует тот факт, что *единственный*

массив $R(0..n)$ достаточен для вычисления полиномов R_{m+k}. Действительно, переход от R_{m+k} к R_{m+k-1} происходит покоэффици- ентно (см. рекуррентную формулу, фигурирующую в доказательстве).

Этот алгоритм деления, разумеется, позволяет реализовать алгоритм Евклида для многочленов, который в любом случае больше не представляет затруднений.

4.2. Неприводимые многочлены с коэффициентами из $\mathbb{Z}/p\mathbb{Z}$

Согласно общим определениям раздела 1, неприводимым многочленом в $K[X]$ является многочлен степени $n \geq 1$ (т.е. не являющийся константой), не имеющий делителя степени, строго меньшей п (кроме постоянных величин, понятно). Следующий параграф уточняет строение неприводимых многочленов в $\mathbb{F}_p[X]$, где $\mathbb{F}_p$ (для простого p) обозначает поле $\mathbb{Z}/p\mathbb{Z}$ целых чисел по модулю p. Докажем существование (в неявном виде) неприводимого многочлена по модулю p произвольной степени. В качестве извинения за отсутствие эффективности в следующем разделе даются критерий неприводимости многочлена и его применения в нескольких конкретных примерах.

Если Q — неприводимый многочлен, то уже показано, что фактор- кольцо $K[X]/(Q)$ является полем (предложение 22). Обозначение (Q) использовано для идеала, порожденного многочленом Q. Этот результат является *фундаментальным*, поскольку является ключевым инструментом в конструировании под полей. Вот несколько уточнений структуры $K[X]/(Q)$.

***Предложение* 6**

Пусть Q — многочлен степени n с коэффициентами в поле K. Тогда факторкольцо $K[X]/(Q)$ есть векторное K-пространство размерности n. Если Q неприводим, то это — поле. Если дополнительно K — конечное поле, состоящее из к элементов, то $K[X]/(Q)$ будет полем, состоящим из k^n элементов.

(Основная часть доказательства состоит в том, чтобы убедиться, что $\overline{1}$, $\overline{X}$, ..., $\overline{X}$K[X]/(Q)).

***Теорема* 7**

Пусть p — простое число из $\mathbb{N}$ и $n \in \mathbb{N}^*$. Для неприводимого многочлена Q из $\mathbb{F}_p[X]$ выполнено: $Q|X^n - X \Leftrightarrow deg\ (Q)|n$.

Доказательство.

Пусть K — факторкольцо $\mathbb{F}_p[X]/(Q)$ и $d = \deg(Q)$. То, что K — конечное поле характеристики p, состоящее из p^d элементов, проверяется известным способом. Обозначим через $\overline{X}$ образ X в K. Мультипликативная группа K^* состоит из p^d—1 элементов, удовлетворяющих соотношению

$$y^{p^d-1} = 1, \text{ для любого } y \in K^* \tag{4}$$

Сначала докажем импликацию «⇐» («только тогда»), предполагая, что $d|n$. Это последнее свойство приводит к тому, что p^d—1 делит p^n—1. Затем с помощью равенства из предыдущего параграфа, примененного к $y = \overline{X}$, получаем: $\overline{X}^{p^n-1} = 1$, откуда $\overline{X}^{p^n} = \overline{X}$. Это последнее равенство в K интерпретируется в $\mathbb{F}_p[X]$ следующим образом:

$$X^{p^n} - X \equiv 0 \,(\mathrm{mod}\, Q) \;\Rightarrow\; Q|X^{p^n} - X,$$

что и дает нужное заключение.
Доказательство импликации «⇒» требует большего внимания. Предположим, что $Q|X^{p^n} - X$. Тогда $X^{p^n} - X \equiv 0 \pmod{Q} \to \overline{X}^{p^n} = \overline{X}$. Но всякий элемент $y \in K$ представим в виде $R(\overline{X})$, где R — многочлен с *коэффициентами* из $\mathcal{O}_p$. Используя теперь тот факт, что поле K имеет характеристику p, заключаем: для всякого $y \in K$ выполнено: $y^{p^n} = R(\overline{X})^{p^n} = R(\overline{X}^{p^n}) = R(\overline{X}) = y$, откуда:

$$y^{p^n-1} = 1, \ \forall y \in K^* \tag{5}$$

Поделим n на d: $n = dq + r$ с $0 \le r < d$. Тогда имеем равенство $p^n - 1 = (p^{dq} - 1)p^r + p^r - 1$, которое ввиду равенств (4) и (5) дает: $y^{p^r-1} = 1$ для любого $y \in K^*$. Многочлен $R(Y) = Y^{p^r-1} - 1 \in K[Y]$ имеет степень $p^r - 1 < p^d - 1$, но обладает $p^d - 1$ корнями в K. Значит, это нулевой многочлен, откуда $p^r - 1 = 0$, т.е. $r = 0$. В этом случае $d|n$, что и требовалось.

■

Теорема 35 дает возможность найти число *унитарных неприводимых* многочленов степени n над полем $\mathbb{F}_p$ (целых чисел по модулю p).

***Следствие* 8**

Пусть I_p^n– число неприводимых унитарных многочленов в $\mathbb{F}_p[X]$ степени n.

(i) $p^n = \sum_{d|n} dI_p^d$.

(ii) $I_p^n \geq 1$ *для всякого простого числа* p *и всякого натурального* n. *Другими словами, для любого натурального* n *существует неприводимы над* $\mathbb{F}_p$ *многочлен степени* n.

Доказательство.

Многочлен $X^{p^n}-X \in \mathbb{F}_p[X]$ не имеет сомножителей, являющихся полными квадратами. Действительно, если $X^{p^n}-X = U^2V$, то, находя производную от обеих частей, получаем: $-1 = 2UU'V + U^2V = U(2U'V + UV')$, откуда следует, что U — константа.

Теорема 35 утверждает, что унитарные неприводимые многочлены Q с $\deg(Q)|n$ являются неприводимыми унитарными делителями $X^{p^n}-X$. Вышеприведенное рассуждение показывает, что эти многочлены появляются роено один раз в простом разложении $X^{p^n}-X$. Следовательно,

$$X^{p^n} - -X = \prod_{d|n} \prod_{Q \in K_p^d} Q$$

где K_p^d обозначает множество неприводимых унитарных многочленов степени d над $\mathbb{F}_p$. Приравнивая степени в левой и правой частях равенства, получаем $p^n = \sum_{d|n} dI_p^d$, что доказывает (*i*).

Для доказательства (*ii*) заметим, что

$$p^d = \sum_{d|n} eI_p^e = dI_p^d + \sum_{e|d} eI_p^e \geq dI_p^d.$$

Следовательно,

$$p^n = \sum_{d|n} dI_p^d = nI_p^n + \sum_{d|n} dI_p^d \leq nI_p^n + \sum_{d|n} p^d \leq$$

$$\leq nI_p^n + \sum_{d=0}^{n-1} p^d \leq nI_p^n + \frac{p^n-1}{p-1}$$

или еще $nI_p^n \geq p^n - \frac{p^n-1}{p-1} \geq 1$, что и требовалось.

■

Вычисление количества неприводимых унитарных многочленов степени n по модулю

Из предыдущего следствия немедленно вытекает (для простого), что $I_p^1 = p, I_p^2 = p(p—1)/2, I_p^3 = p(p^2—1)/3$ и вообще для **простого** n: $I_p^n = p(p^{n-1}-1)/n$.

Из формулы, доказанной в предыдущем следствии, можно получить рекуррентное соотношение, позволяющее найти I_p^n для произвольного n:

$$I_p^n = \frac{1}{n}(p^n - \sum_{d|n} dI_p^d).$$

В таблице 2 приведены значения I_p^n (полученные, разумеется, с помощью Ада-программы) для p = 2,3,5,7 и n от 1 до 10.

p	I_p^1	I_p^2	I_p^3	I_p^4	I_p^5	I_p^6	I_p^7	I_p^8	I_p^9	I_p^{10}
2	2	1	2	3	6	9	18	30	56	99
3	3	3	8	18	48	116	312	810	2184	5880
5	5	10	40	150	624	2580	11160	48750	217000	976248
7	7	21	112	588	3360	19544	117648	720300	4483696	28245840

Таблица 2: Число неприводимых многочленов по модулю p

Замечание. 976 248 неприводимых многочленов степени 10 над F^5 дают 976 248 полей вычетов, каждое из которых состоит из $5^10 = 9765625$ элементов. В действительности (это классический результат теории конечных полей) все они изоморфны. Другими словами, поле с таким числом элементов всегда одно! Более точно, для каждой степени q простого числа существует единственное конечное поле, состоящее из q элементов (см. упр. 57).

Применение формулы обращения Мёбиуса (раздел 6.3) к формуле (i) следствия 36 сразу же дает

Следствие 9

Если μ — обычная функция Мёбиуса, то, сохраняя введенные выше обозначения, имеем:

$$I_p^n = \frac{1}{n}\sum_{d|n} \mu(d)p^{n/d}.$$

4.3. Простой критерий неприводимости по модулю p

Переформулировка теоремы 35 позволяет дать критерий неприводимости по модулю . Этот критерий применяется к полиномам степени n, где n превосходит p и число p мало. Существует другой, эффективный критерий неприводимости по модулю p, принадлежащий Берлек- эмпу [21].

***Следствие* 10**

Пусть p —простое натуральное число, $Q \in \mathbb{F}_p[X]$ имеет степень n. Q неприводим тогда и только тогда, когда для любого простого делителя q числа n выполнено:

$$Q|X^{p^n} - X \text{ и } НОД(X^{p^{n/q}} - X.Q) = 1.$$

Доказательство.

Допустим, что Q неприводим. По теореме 35 $Q|X^{p^n}$—X и $Q \nmid X^{p^m}$—X, если m — собственный делитель n (т.е. $n \nmid m$), что доказывает первую половину следствия.
Допустим, что выполнены условия доказываемого критерия и R — неприводимый множитель Q. Тогда $R|X^{p^n}$—X и $R \nmid X^{p^n}$—X для любого простого делителя q числа n. Используя теорему 35, имеем: $\deg(R)|n$ и $\deg(R) \nmid n/q$ для любого простого делителя q числа n. Отсюда следует, что $\deg(R) = n$ и потому $R \sim Q$. Следовательно, Q — неприводимый многочлен.

■

Замечание. При реализации этого теста советуем работать в кольце $\mathbb{F}_p[X]/(Q)$ (элементы которого могут быть представлены массивами длины n) и вычислять X^{p^i} с помощью дихотомического алгоритма. Можно использовать также тот факт, что отображение $\Phi : x \mapsto x^p$ является линейным отображением $\mathbb{F}_p[X]/(Q)$ (допускающим кодирование при помощи матрицы размера $n \times n$) и тогда $X^{p^i} = \Phi^i(X)$.

Некоторые примеры тестов на неприводимость

1. Пусть многочлен $Q(X) = X^{10}+X^3+1$ из $\mathbb{F}_2[X]$. Согласно критерию, приведенному выше ($n =$deg$(Q) = 10$ и $q = 2,\ 5$), имеем $(X^{2^10} - X) \bmod Q(X) = 0$, но НОД$(X^{2^5} - X, Q(X)) = 1$ для $q = 2$ и, наконец, НОД$(X^2$—$X, Q(X)) = 1$ для $q = 5$. Следовательно, полином $Q(X) = X^{10} + X^3 + 1$ неприводим по модулю 2.

2. Пусть многочлен $Q(X) = X^5 + X^4 + X^3 + X^2 + X - 1$ из $\mathbb{F}_3[X]$. Критерий, описанный выше, дает $(X^3 — X) \bmod Q(X) = — X^2 — X — 1$. Этот результат достаточен для того, чтобы утверждать, что многочлен не является неприводимым. Второй шаг проверки, нахождение НОД$(X^3 — X, Q(X)) = 1$ при $q = 5$ не требуется. Впрочем, тест не позволяет найти ни одного *делителя* Q. ■

Итак, теперь мы знаем два основных примера евклидовых колец: $\mathbb{Z}$ и $K[X]$ (K — поле), которые имеют, с точки зрения деления, одинаковое поведение. В частности, эти два кольца обладают тем важным свойством, сформулированным в предложении 31, что все их идеалы главные. Действительно, это свойство (как будет показано в следующем разделе) — единственное достаточное условие для выполнения основной теоремы арифметики.

5. Кольца главных идеалов или идеалистическая точка зрения

Работа математика заключается, между прочим, в изучении гипотез, имеющих важные последствия. Примером служит ситуация, встретившаяся здесь. Если читатель внимательно прочитал доказательства результатов раздела 4, то заметил, что свойство «всякий идеал главный» действительно становится главным (кроме, разумеется, предположений о целостности, т.е. отсутствия делителей нуля).

5.1. Идеализация

Математик идеализирует ситуацию следующим образом:

***Определение* 11** (кольцо главных идеалов)
Кольцо A называется кольцом главных идеалов (КГИ), если оно без делителей нуля и всякий его идеал главный.

Понятие кольца главных идеалов определяет новый класс факториальных колец, удовлетворяющих (не эффективным образом) соотношению Везу и строго содержащих класс евклидовых колец без делителей нуля:

***Предложение* 12**
Кольцо главных идеалов A факториально и удовлетворяет соотношению Везу.

Доказательство.

Из того, что всякий идеал в A главный следует, с одной стороны, что A нётерово, а с другой, что A — кольцо Безу. Согласно полученным в разделах 2.1 и 2.4 результатам (предложения 9, 10 и 20), А факториально, что равносильно свойству Безу.

■

Замечание. Из того, что A — КГИ следует, что для любых a и $b \in A$ существует наибольший общий делитель (НОД) d этих элементов (задающийся равенством $Aa + Ab = Ad$) без способа вычисления этого НОД (в отличие от евклидовых колец). Арифметические свойства евклидовых колец и колец главных идеалов, в основном, те же: явное различие между этими двумя категориями заключается в исчислении объектов. Надо все-таки отметить, что существуют неевклидовы кольца главных идеалов, для которых имеются алгоритмы вычисления НОД и даже коэффициентов Безу (например, некоторые кольца квадратичных расширений кольца целых чисел, квадратичных полей, см. упр. 59).

***Предложение* 13**

Классы колец, введенных к настоящему моменту, связаны следующими включениями:

$$\left\{\begin{array}{l}\text{Евклидовы кольца}\\ \text{без делителей нуля}\end{array}\right\} \subsetneq \left\{\begin{array}{l}\text{Кольца главных}\\ \text{идеалов}\end{array}\right\} \subsetneq \left\{\begin{array}{l}\text{Факториальные}\\ \text{кольца}\end{array}\right\}.$$

Доказательство.

Единственная проблема состоит в том, чтобы показать, что указанные тут классы различны. Чуть позже в этой главе, мы покажем, что кольцо многочленов с целыми коэффициентами $\mathbb{Z}[X]$ факториально. Докажем сейчас, что не все идеалы в $\mathbb{Z}[X]$ являются главными. Рассмотрим, например, идеал $(X)+(2)$ и предположим наличие образующего элемента P для $(X)+(2)$. Тогда $2 \in (P)$, и P делит 2. Итак, $P = \pm 2$ или $P = \pm 1$. Возможность $P = \pm 2$ приводит к противоречию, так как $X \notin (2)$. Что касается другой возможности $P = \pm 1$, то она приводит к существованию полиномов $U(X)$ и $V(X)$ из $\mathbb{Z}[X]$, таких, что $1 = U(X) \times X + V(X) \times 2$. Подставив в последнее тождество $X = 0$, получим $1 = 2V(0)$, что абсурдно. Итак, $\mathbb{Z}[X]$ не КГИ. Существование КГИ, не являющегося евклидовым, более деликатная проблема и, как обычно, предоставляется читателю (упр. 21).

Приведем здесь только два известных кольца, являющихся КГИ, но не евклидовыми. Первое — кольцо целых чисел из $\mathbb{Q}[\sqrt{-19}]$:

$$A = \mathbb{Z} + \frac{1+\sqrt{-19}}{2}\mathbb{Z} = \{\frac{x+y\sqrt{-19}}{2}, \text{ где } x \equiv y \pmod 2\},$$

Второе — факторкольцо $M[X,Y]/(X^2+Y^2+1)$.

■

5.2. Частные кольца главных идеалов

Так как КГИ A является кольцом Безу, то всякий идеал, порожденный неприводимым элементом $q \in A$, максимален (т.е. факторкольцо $A/(q)$ есть тело). Это видно из предложения 22. Классические примеры: $\mathbb{Z}/p\mathbb{Z}$ и $K[X]/(P)$. Следующее предложение обобщает этот результат, описывая обратимые элементы всякого факторкольца $A/(q)$, результат совершенно аналогичный описанию известного факторкольца $\mathbb{Z}/n\mathbb{Z}$.

***Предложение* 14**
В кольце главных идеалов понятия максимального, простого или неприводимого элементов совпадают. Пусть q не является ни нулевым, ни обратимым в кольце A.

(i) Пусть x — элемент A. Тогда $\overline{x}$ обратим в $A/(q)$ тогда и только тогда, когда x и q взаимно просты, равносильным образом, существуют такие u и v, что $ux+vq=1$.

(ii) В частности, $A/(q)$ — тело тогда и только тогда, когда q является неприводимым элементом A.

Доказательство.

Пусть d является НОД q и x, а u и v — коэффициентами Безу; q и x взаимно просты, т.е. $d=1$. Отсюда следует (i). Эквивалентности:

$$\overline{ux} = 1 \text{ (в } A/(q)) \quad \Leftrightarrow \quad ux \equiv 1 \pmod{q} \quad \Leftrightarrow \quad ux \in 1 + Aq$$

заканчивают доказательство первого из утверждений. Второе те- перь становится очевидным.

■

Примеры

Предыдущее предложение может рассматриваться как инструмент, позволяющий строить тела с помощью перехода к частному. Вот несколько элементарных примеров, в основе которых лежит этот фундаментальный принцип.

1. Каждое простое число p порождает поле $\mathbb{Z}/p\mathbb{Z}$ вычетов по модулю p. Кроме того, всякое простое p, сравнимое с 3 по модулю 4, неприводимо в $\mathbb{Z}[i]$ (предложение 8) и, следовательно, порождает поле $\mathbb{Z}[i]/p\mathbb{Z}[i]$, имеющее p^2 элементов. Например, $\mathbb{Z}[i]/7\mathbb{Z}[i]$ есть поле из 49 элементов. Эти элементы записываются в виде $a + \bar{i}b$, где a и b в $\mathbb{Z}[i]/7\mathbb{Z}[i]$ и $\bar{i}$ (элемент факторкольца) удовлетворяет соотношению $\bar{i}^2 = —1$.

2. Рассмотрим многочлен $X^3 + X + 1$ с коэффициентами из $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Это неприводимый многочлен (можете проверить), что позволяет построить поле $K = \mathbb{F}_2[X]/(X^3 + X + 1)$ порядка 8, элементы которого имеют вид $a\alpha^2 + b\alpha + c$, где a, b, $c \in \mathbb{Z}/2\mathbb{Z}$ и a (элемент факторкольца) удовлетворяет соотношению $\alpha^3 = —\alpha—1$.

6. Об оптимальных алгоритмах вычисления НОД

В предыдущих разделах мы рассмотрели алгоритм Евклида и различные математические понятия для его выражения. Чтобы закончить обсуждение, необходимо оценить сложность алгоритма Евклида в нескольких особых случаях и наметить способы получения оценок для более общих ситуаций. Первые оценки сложности алгоритма Евклида принадлежат Ламе [109] и являются предметом изучения первой части этого раздела. Эта теория проста и вполне доступна студенту первого курса университета, но заставляет прибегнуть к последовательности Фибоначчи.

Эта теория также провоцирует вопрос: «существуют ли оптимальные алгоритмы вычисления НОД?» и приводит к появлению понятий квазиевклидова кольца и квазиалгоритма. Наконец, теорема Дирихле порождает идею плотности пар целых простых чисел, полезная вещь для тех, кто хочет вычислять НОД более чем двух целых чисел.

6.1. Вычисление НОД двух целых чисел: теорема Ламе

Используемые обозначения те же, что и в предыдущих разделах. Пусть a и b — два натуральных числа, для которых необходимо вычислить НОД. Как обычно, алгоритм Евклида позволяет построить последовательность $(r_i)_{0\leq i\leq n+1}$:

$$r_0 = a,\ r_1 = b \text{ и } r_{i-1} = r_i q_i + r_{i+1},$$

где $0 < r_{i+1} < r_i$ для $1 \leq i < n$, а $r_{n+1} = 0$,

последнее деление $r_{n-1} = r_n q_n$ является делением нацело. В этих условиях алгоритм Евклида требует n итераций для своей реализации (используемое деление — обычное деление натуральных чисел).

***Определение* 15**

Последовательностью Фибоначчи $(F_n)_{n\in\mathbb{N}}$ *называется последовательность, задаваемая следующим образом:* $F_0 = 0, F_1 = 1$ *и для* $n \geq 0 F_{n+2} = F_{n+1} + F$

> **Замечание.** Эта последовательность названа в честь итальянского математика начала XIII века Леонардо Фибоначчи, который использовал ее при подсчете размножения кроликов (1202 г.), см. Кнут [97]. Эта последовательность естественным образом возникает при изучении процесса роста листвы некоторых растений. Числа Фибоначчи связаны с золотым сечением через соотношение $F_p = (\phi^p — \hat{\phi})/\sqrt{5}$, где ϕ — положительный корень уравнения (называемый золотым числом) $X^2 — X — 1 = 0$, $\phi = (1 + \sqrt{5})/2$ и $\hat{\phi} = (1 - \sqrt{5})/2$.

В данном исследовании для простоты предполагается, что $a > b$. Если это не выполнено, то легко видеть, что первое деление, выполненное по алгоритму Евклида, меняет ролями а и 6 и приводит нас именно к этому предположению.

Прежде чем формулировать теорему Ламе, установим несколько простых свойств, позволяющих сделать ее доказательство более естественным.

***Свойство* 16**

Если для того, чтобы вычислить НОД чисел a и b, таких, что $a > b > 0$ *алгоритм Евклида требует n итераций, то* $a \geq F_{n+2}$ *и* $b \geq F_{n+1}$. *Если к тому же* $a = F_{n+2}$ *и* $b = F_{n+1}$, *то алгоритм Евклида требует ровно n итераций для вычисления НОД(a, b) (их наибольший общий делитель равен 1).*

Доказательство.

Прежде всего заметим, что $r_n \geq 1$ (в противном случае последнее деление дает нулевой остаток). Кроме того, $r_n < r_{n-1}$ и, следовательно, $r_{n-1} \geq 2$, откуда $r_n \geq F_2$ и $r_{n-1} \geq F_3$ (напомним: $F_2 = 1$ и $F_3 = 2$
С другой стороны, при делении $r_{i-1} = r_i q_i + r_{i+1}$ частное q_i нулевое и потому $r_{i-1} \geq r_i + r_{i+1}$. С помощью нисходящей индукции можно доказать, что $r_i \geq F_{n+2-i}$ для $0 \leq i \leq n$, что и доказывает сформулированное свойство.
Чтобы доказать вторую часть, достаточно в явном виде продолжить последовательность делений: $F_{n+2} = F_{n+1} + F_n$, $F_{n+1} = F_n + F_{n-1}, \ldots$ и, наконец, $F_3 = F_2 \times 2$ (действительно, $F_2 = F_1 = 1$). Отсюда следует, что НОД$(F_{n+2}, F_{n+1}) = F_2 = 1$, и что необходимо ровно п итераций для реализации алгоритма Ев- клида на этой паре чисел.

■

***Свойство* 17**

В предположении, что алгоритм Евклида требует n итераций, справедливы соотношения:

$$n+2 < \frac{\log_{10}\sqrt{5}(a+1)}{\log_{10}\phi} \text{ и } n+1 < \frac{\log_{10}\sqrt{5}(b+1)}{\log_{10}\phi}.$$

Доказательство.

Для доказательства этих соотношений достаточно сопоставить предыдущее свойство с соотношением, связывающим ϕ и F_n, приведенное в предыдущем примечании, зная, что $|\hat{\phi}| < 1$. Например,

$$a \geq F_{n+2} \Leftrightarrow a \geq \frac{1}{\sqrt{5}}(\phi^{n+2} - \hat{\phi}^{n+2}) \Rightarrow$$

$$\Rightarrow a > \frac{1}{\sqrt{5}}(\phi^{n+2} - 1) \Rightarrow a + 1 > \frac{\phi^{n+2}}{\sqrt{5}}. \quad (6)$$

■

***Теорема* 18** (Ламе)

Число итерации, необходимых для вычисления НОД двух натуральных чисел a и b, таких, что $a > b > 0$, мажорируется 5-кратным числом десятичных знаков наименьшего из этих двух чисел. Более формально, если n является искомым числом итерации, то

$$n \leq 5(\lfloor \log_{10} b \rfloor + 1) \text{ или } n \leq 5\lceil \log_{10}(b+1) \rceil.$$

***Лемма* 19**

Пусть p — число десятичных цифр положительного целого числа b. Тогда

$$\lfloor \frac{\log_{10}\sqrt{5}(b+1)}{\log_{10}\phi} \rfloor \leq 5p + 1.$$

Доказательство.

По условию $b \le 10^p - 1$ и $log_{10} b + 1 \le p$. Следовательно,

$$\frac{\log_{10}\sqrt{5}(b+1)}{\log_{10}\phi} = \frac{\log_{10}(b+1)}{\log_{10}\phi} + \frac{\log_{10}\sqrt{5}}{\log_{10}\phi} \le \frac{1}{log_{10}\phi} p + \frac{\log_{10}\sqrt{5}}{\log_{10}\phi} = \alpha p + \beta$$

так как $\alpha \approx 4,7849$ меньше 5 и $\beta 1,6722$ несколько меньше 2. Итак, можно записать: $\alpha p + \beta = 5p + \beta - (5 - \alpha)p$, формула, в которой число $(\beta$—$(5$—$\alpha)p$ мажорируется 1, когда $p \ge 4$, что дает

$$\frac{\log_{10}\sqrt{5}(b+1)}{\log_{10}\phi} \le \alpha p + \beta \le 5p + 1.$$

Чтобы завершить доказательство, остается рассмотреть случаи, когда $p = 1$,2 или 3. Простые вычисления показывают, что когда $p \in [1, 3]$, имеем $\lfloor \alpha p + \beta \rfloor = 5p + 1$, что доказывает лемму.

■

Доказательство (теоремы Ламе).

Свойство 45 вместе с предыдущей леммой позволяет без труда доказать теорему Ламе. Действительно, из этих двух результатов выводим $n + 1 \le 5p + 1$, т.е. $n \le 5p$. Кроме того, утверждение, состоящее в том, что b имеет p десятичных цифр в записи, означает $p = \lfloor \log_{10} b \rfloor + 1 = \lceil \log_{10}(b+1) \rceil$.

■

Главный результат в этой теории — сложность алгоритма Евклида для целых чисел логарифмическая по отношению к наименьшему из двух чисел. (Обозначение $O(\log b)$ скрывает весьма существенную константу).

Замечание. В оценке Ламе коэффициент 5 оптимален, так как для следующих пар (13,8), (144,89) и (1597,987), соответствующих парам (F_7, F_6), (F_{12}, F_{11}) и (F_{17}, F_{16}), число итераций алгоритма Евклида, соответственно, 5, 10 и 15. Впрочем, это свойство не идет дальше F_{17} и F_{16}. Действительно, для пары

$$(F_{22},\ F_{21}) = (17711,\ 10946)$$

число итераций равно 20, в то время как оценка Ламе 25. Это показывает, что если коэффициент 5 оптимален, то мажорирующая функция таковой не является.