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. остат**
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	$12 = -6 \times -2 + 0$		

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.

(29) Лемма.

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 $\tilde{\varphi}(1) = \min\{\varphi(a) | a \in I \backslash 0\}$ — 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.

(30) Предложение.

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 $^* \backslash U(A)$ 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.

(31) Предложение.

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 1 *Можно заметить, что в $\mathbb{Z}$ или в [] 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)

(32) Теорема (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.

(33) Следствие.

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 $K[X]/(Q)$.

(34) Предложение.

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)).

(35) Теорема.

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 $\mho_p$. 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).

(36) Следствие.
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 от1 до10.

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

(37) Следствие.

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

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