Доказательство.

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

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

так как $\alpha \approx 4,7879$ меньше 5 и $\beta \approx 1,6722$ 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 $p \geqslant 4$, что дает

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

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 $n + 1 \leqslant 5p + 1$, т.е. $n \leqslant 5p$. 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 числе логарифмическая по отношению к наименьшему из двух чисел. (Обозначение $O(logb)$ 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 по казывает, что если коэффициент 5 оптимален, то мажорирующая функция таковой не является.

0.1. Квазиевклидовы кольца

Мы только что доказали, что оценка, даваемая теоремой Ламе, опти маль- на только в некоторых особых случаях. Но даже если бы выраже ние, да- ваемое этой теоремой, было наилучшим, вопрос об оптимально сти алго- ритма Евклида нахождения НОД двух целых чисел все равно остался бы. Действительно, обычное евклидово деление не приводит к оптимально- му алгоритму Евклида, как видно из раздела 3.4. Цель данного раздела — найти деления, которые оптимизируют сложность этого алгоритма. До настоящего момента мы рассматривали, главным образом, три класса ко- лец, связанные следующими включениями:

$$hzhzhzhhzhz$$

Главные их характеристики, которые нас интересуют, следующие:

- *Наличие* алгоритма Евклида и возможность эффективного вычи сле- ния НОД. Прототипами евклидовых колец являются $\mathbb{Z}$ и мно жество многочленов над полем.

- *Наличие* НОД и разложения Безу без эффективного метода вы числе- ния. Кольцо целых чисел из $\mathbb{Q}\sqrt{-19}$ является неевклидо вым кольцом главных идеалов, в котором, между прочим, суще ствует метод вы- числения коэффициентов Безу [141] (кольцо целых $\mathbb{Q}\sqrt{-19}$, состоящее из элементов, которые являются корнями унитарных многочленов с коэффициентами из $\mathbb{Z}$).

- *Наличие* и *единственность* разложения на простые множители (ос- новная теорема арифметики). Кольцо $A[X]$ многочленов с ко эффици- ентами из A факториально, если таковым является A, но не является КГИ, если A не является телом.

Хотя понятие евклидова кольца более интересное с точки зрения эф- фективности, понятие алгоритма Евклида значительно сильнее. На прак- тике оно ограничено методами, которые были представлены выше:

- В КГИ известно существование НОД, но нет, вообще говоря, про стой эффективной процедуры его вычисления.

- Как будет видно из следующей главы, посвященной модулям над КГИ, что является основным содержанием главы, важным явля ется не вы- числение НОД с помощью деления, а вычисление коэф фициентов Везу (что, конечно, приводит к нахождению НОД).

- В кольце главных идеалов наличие НОД зависит не столько от то го, что всякий идеал главный, сколько от того, что он конечного типа (этого достаточно).

- Наконец, как показывают нижеследующие результаты, сходи мость некоторого метода такого, как алгоритма Евклида, не обя зательно связано с существованием алгоритма Евклида в рассма триваемом кольце.

(48) Определение.

Пусть A — коммутативное унитарное кольцо. **Квазиалгоритм** *на A есть отображение φ множества A x A во вполне упорядоченное мно жество, обладающее следующим свойством:*

$$\forall (a,b) \in A \times A^*, \exists (q,r) \in A \times A \text{ *такая, что* } a = bq + r \text{ и } \varphi(b,r) < \varphi(a,b)$$

Это равенство называется делением a на b. Кольцо A называется **квазиевклидовым,** *если оно допускает квазиалгоритм φ. Говорят также, что A квазиевклидово относительно φ*

> **Примечание.** Так как в случае евклидовых колец, термин *алгоритм* обозначал отображение, а не эффективный метод вычисле ния, то квазиалгоритм также будет полностью формальным объ ектом. Эта терминология нежелательна в работе, которая рас сматривает алгоритмы в «информатическом» смысле.

(49) Предложение.

(i) Всякое евклидово кольцо является квазиевклидовым.

(ii) В квазиевклидовом кольце всякий идеал конечного типа главный (что приводит к наличию НОД двух элементов). Это означает, что всякое квазиевклидово кольцо является кольцом Везу.

(iii) В частности, всякое нётерово квазиевклидово кольцо без дели телей нуля является КГИ (в нётеровом всякий идеал конечного типа).

Доказательство. только для (*ii*)

> Пусть идеал порожден двумя элементами. Допустим, что $(a,b) \in A \times A$ — пара образующих идеала $I, I = Aa + Ab$, где b отличен от нуля, для которой φ имеет наименьшее значение. Мож но осуществить квазиевклидово деление a на b и записать $a = bq + r$, где $\varphi(b,r) < \varphi(a,b)$. Это приводит, в частности, к $Aa + Ab = Ab + Ar$ и противоречит выбору пары (a,b). Следовательно, такой пары с $b \neq 0$ не существует, т.е. $b = 0$. Это запускает механизм индукции, которая не вызывает особых трудностей. Наличие НОД теперь вы водится из того, что $Ad = Aa + Ab \Rightarrow [\delta | d \iff \delta | a$ и $\delta | b]$.

Замечание. Конечно, лучшее понимание квазиевклидова деле ния, основного для вычисления НОД, необходимо. Однако оно не позволяет провести эти вычисления. Как показывает преды дущее доказательство, НОД двух элементов кольца определяется единственным образом (это нулевой элемент пары, порождающий сумму идеалов, для которой значение квазиалгоритма минималь но, что не является эффективным средством вычисления).

Алгоритм Евклида остается допустимым для квазиевклидовых ко лец и обладает той же сходимостью, что и в евклидовых кольцах.

(50) Предложение.

Коммутативное унитарное кольцо A является квазиевклидовым то гда и только тогда, когда оно удовлетворяет следующему условию:

$$\forall (r_0, r_1) \in A \times A, \exists n \in \mathbb{N}, \exists (q_1, \ldots, q_n) \in A^n, \exists (r_2, \ldots, r_{n+1}) \in A^n,$$
$$\textit{такие, что: } \forall i \in [1, n] : r_{i-1} = r_i q_i + r_{i+1} \text{ и } r_{n+1} = 0.$$

Кроме того, отображение φ которое со всякой парой $(r_0, r_1) \in A \times A$ ассоциирует наименьшее целое n, для которого существует цепь псев до делений, оканчивающаяся нулевым остатком, является самым малым квазиалгоритмом, определенным на A.

Доказательство.

Согласно второму пункту предшествующего замечания, условие не обходимо. Поэтому надо показать его достаточность. Итак, пусть A — кольцо, удовлетворяющее условию предложения 50. Ясно, что отображение φ есть квазиалгоритм для A. Действительно, пусть a, b и r такие, что минимальная цепь псевдо делений для пары (a, b) начинается с $a = bq+r$. Тогда, принимая во внимание минимальность φ, имеем $\varphi(b, r) + 1 \leqslant \varphi(a, b)$ и, следовательно, $\varphi(b, r) < \varphi(a, b)$. Проверка того, что указанный квазиалгоритм минимален, является простой формальностью.

Итак, данное предложение позволяет построить квазиалгоритм для квазиевклидова кольца. Это построение (если оно эффективно) опре деляет самый быстрый метод вычисления НОД через алгоритм «по в клиду» в квазиевклидовом кольце. Действительно, Лазар [112] доказал следующие свойства:

(51) Теорема (Лазара)

(i) Обычное евклидово деление в K[X] является евклидовым делени ем, согласно минимальному квазиалгоритму в K[X]. Алгоритм Евкли да, сле-

довательно, является самым быстрым методом вычисления НОД двух многочленов с коэффициентами в поле через последовательные деления.

(ii) В $\mathbb{Z}$ всякое евклидово деление с самым малым остатком является делением согласно минимальному кваэиалгоритму в $\mathbb{Z}$.

(iii) Точнее, в $\mathbb{Z}$ деление $a = bq + r$ есть деление по минимальному квазиалгоритму тогда и только тогда, когда $|r| < |b|/\phi$ (ϕ является золотым числом и $1/\phi \approx 0,6180339\ldots$).

Доказательство.

Доказательство пункта (i) очень простое и фигурирует в упражне ниях 42 и 43, находящихся в конце главы. Пункты (i) и (iii) не очень интересны для доказательства и не представляют больших трудно стей. Например, можно проиллюстрировать пункт (iii). Пусть для вычисления НОД даны числа 4215 и 1177. Вот различные этапы ал горитма Евклида. Слева используется деление с наименьшим остат ком, а справа деление, для которого отношение остатка к частному может превысить 0,5, все еще не превышая $1/\phi$:

$$hzhzhzhz$$

В решении по этому последнему алгоритму 4 деления, отмеченные звездочкой, дают остатки, абсолютное значение которых больше половины делителя, оставаясь в границах теоремы Лазара, а число итераций остается равным 9 (значение минимального квазиалго ритма для этих двух целых чисел).

0.2. Вычисление НОД нескольких целых чисел: теорема Дирихле

Когда необходимо вычислить НОД нескольких чисел, а не только двух, можно применить несколько методов:

• Распространение алгоритма Евклида, базирующегося на следую щих свойствах: *(i)* НОД$(0,\ldots,0,a,0,\ldots,0)=a$, *(ii)* НОД$(u_1,\ldots,u_i,\ldots,u_n)$ = НОД$(u_1$ mod $u_i,\ldots,u_i,\ldots,u_n$ mod u_i) при $u_i \neq 0$. За подробностями этого метода читатель может обратиться к упр. 24.

• Следующий метод заключается в повторном применении алгорит ма Евклида для двух целых чисел. Он основывается на следую щем свойстве: НОД$(u_1,\ldots,u_n)$ = НОД$(u_1$,НОД$(u_2,\ldots,u_n)$), ко торое порождает рекурсивный алгоритм вычисления НОД. Имен но, НОД$(u_1,\ldots,u_n)$ = НОД(НОД$(u_1,\ldots,u$ что являет ся основой соответствующего итеративного алгоритма.

Этот последний метод не только упрощает реализацию вычисле ния — действительно, достаточно несколько раз применить уже реа лизованный алгоритм — но и имеет неоспоримое достоинство с точки зрения эффективности. Неформально говоря, главное заключается в следующем: выбирают два числа в последовательности, для которой надо вычислить НОД. Затем, сделав первое вычисление, заменяют два выбранные числа на их НОД и повторяют алгоритм. Выигрыш в эф фективности получается из того, что как только находят НОД, рав ный единице, вычисление может быть прервано. Неиспользованные чи сла ничего не могут добавить к полученным результатам. К тому же это явление довольно распространенное, потому что, как утверждает теория Дирихле, более, чем в 60чайно, взаимно просты. Продолжение этого раздела посвящается двум доказательствам теоремы Дирихле. Одно — эвристическое (короткое и неправильное), а другое — более длинное, но верное. Второе доказа тельство требует введения функции Мёбиуса, и мы воспользуемся слу чаем доказать формулу обращения Мёбиуса — ту формулу, которая уже была использована в разделе 4.2.

(52) Теорема (Дирихле)

Если u *и* v *— два натуральных числа, выбранные случайно, то веро ятность того, что они взаимно просты, равна* $6/sqrt\pi \approx 0,607927$. *Более формально, если*

$H_1^n = \{(u,v) \in \mathbb{N}^{*2}/1 \leqslant u \leqslant n, 1 \leqslant v \leqslant n$ и НОД$(u,v)=1\}$,

то $p = \lim\limits_{n\to\infty} \frac{\#H_1^n}{1} = \frac{6}{sqrtn}$, *где* $\#H_1^n$ *означает мощность множества* H_1^n

Обозначения, использующиеся в следующих ниже доказательствах, таковы. Для натурального числа d и вещественного положительного x определим:

$H_d = \{(u,v) \in \mathbb{N}^{*2}/$ НОД$(u,v) = d\}$,

$H_d^x = \{(u,v) \in \mathbb{N}^{*2}/1 \leqslant u \leqslant x, 1 \leqslant v, \leqslant x$ и НОД$(u,v) = d\}$

В этих обозначениях x часто будет заменяться на натуральное число, как в формулировке теоремы Дирихле. Множество H_1 необходимо для оценки функции распределения в $\mathbb{N}^{*2}$.

Эвристическое доказательство (теоремы Дирихле).

Утверждение НОД$(u,v) = d$ равносильно тому, что u и v кратны d и что НОД$(u/d, v/d) = 1$ (т.е. $(u/d, v/d) \in H_1$). К тому же для всякого натурального n множества H_d^{nd} и H_1^n имеют одну и ту же мощность. Следовательно, для > 0:

$$\frac{\#H_d^x}{x^2} = \frac{\#H_1^{x/d}}{x^2} = \frac{\#H_1^{x/d}}{(x/d)^2} = \frac{\#H_1^{x/d}}{(x/d)^2} \times \frac{1}{d^2}$$

Переходя к пределу, получим:

$$\lim_{x\to\infty} \tfrac{\#H_d^x}{x^2} = \tfrac{1}{d^2} \times \left(\lim_{x\to\infty} \tfrac{\#H_1^x}{x^2}\right) = \tfrac{p}{d^2},$$

где последнее число — «вероятность» того, что два числа имеют наибольший общий делитель d. С другой стороны, можно запи сать $\mathbb{N}^{*2} = \cup_{d=1}^{\infty} H_d$, где объединение является объединением не- пересекающихся множеств (H_d — есть множество пар целых на туральных чисел с НОД равным d). Тогда можно заключить, что $1 = \Sigma_{d=1}^{\infty} p/d^2 = p\Sigma_{d=1}^{\infty} 1/d^2 = p\pi^2/6$.

Настоятельно просим читателя найти ошибку в этом интуитивном доказательстве.

А сейчас переходим к доказательству теоремы Дирихле. Для этого доказательства нужна функция Мёбиуса вне связи с теорией арифме тических функций, где она обычно появляется.

(53) Свойство.

Назовем функцией Мёбиуса функцию μ, определенную на $\mathbb{N}^*$ следу ющим образом:

$$hzhzhzhzhhzhzhzhzhzhz$$

Эта функция тесно связана с частичным упорядочиванием на множе стве целых чисел с помощью отношения делимости. Для целого числа $d > 1$ функция μ удовлетворяет соотношению $\Sigma_{k|d}\mu(k) = 0$.

Доказательство.

Пусть $d = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ — каноническое разложение d. Достаточно рассмотреть только делители d, свободные от квадратов, так как функция μ на других делителях исчезает, т.е. такие делители числа d, которые разлагаются в произведение простых p_i с показателями 0 или 1. Следовательно, чтобы найти такие делители, достаточно выбрать j различных чисел $_i$ и получить

$$\sum_{k|d} \mu(k) = \sum_{j=0}^{r} (-1)^j \times (hzhzhz) = (1 + (-1))^r,$$

согласно определению μ.

Теперь мы получим формулу обращения Мёбиуса в не совсем при вычной форме

(54) Предложение.

Пусть f и g — две функции от $R_+^\bullet$ со значениями в некоторой ад дитивной абелевой группе. Тогда

$$f(x) = \sum_{k=1}^{\lfloor x \rfloor} g\left(\frac{x}{k}\right) \Longleftrightarrow g(x) = \sum_{k=1}^{\lfloor x \rfloor} \mu(k) \times f\left(\frac{x}{k}\right).$$

Доказательство. Используемый метод заключается в перенесении выражения от f, задаваемого первой формулой, во вторую:

$$\sum_{k=1}^{\lfloor x \rfloor} \mu(k) \times f\left(\frac{x}{k}\right) = \sum_{k=1}^{\lfloor x \rfloor} \left(\mu(k) \times \sum_{k=1}^{\rfloor x/k \lfloor} g\left(\frac{x/k}{p}\right)\right) = \sum_{hzhz} \mu(k) \times f\left(\frac{x}{kp}\right).$$

Учитывая, что = $\lfloor \lfloor x \rfloor / k \rfloor = \lfloor x/k \rfloor$, можно сделать следующую замену переменных: $h = kp$ с $1 \leqslant h \leqslant x$ и $k|h$, что дает

$$\sum_{k=1}^{\lfloor x\rfloor} \times f\left(\frac{x}{k}\right) = \sum_{h=1}^{\lfloor x\rfloor}\left(g\left(\frac{x}{h}\right) \times \sum_{k|h} \mu(k)\right).$$

Согласно свойству 53, в этой сумме есть только одно ненулевое сла гаемое, именно то, которое отвечает значению $h = 1$ и, следователь- но $\sum_{k=1}^{\lfloor x\rfloor} \mu(k) \times f(x/k) = g(x)$.

Доказательство теоремы Дирихле будем осуществлять в три этапа.

(55) Лемма.

Пусть x — вещественное положительное число. Обозначим через q_x число элементов множества H_1^x. Тогда $q_x = \sum_{k\geqslant 1} \mu(k) \times \lfloor x/k\rfloor^2$, фор мула, в которой, на первый взгляд, бесконечное число слагаемых, но только конечное их число отлично от нуля.

Доказательство

Пусть $q_{d,x}$ — множество элементов множества H_d^x.Множество пар натуральных чисел, не превосходящих x, есть, как это было видно в эвристическом доказательстве, теоретико-множественная сумма непересекающих подмножеств H_d^x, где d изменяется от 1 до $\lfloor x\rfloor$: $\lfloor x\rfloor^2 = \sum_{d=q}^{\lfloor x\rfloor} q_{d,x} = \sum_{d=1}^{\lfloor x\rfloor} q_{\lfloor x/d\rfloor}$, так как $\#H_d^x = \#H_1^{\lfloor x/d\rfloor}$. При меним к этому выражению формулу обращения, фигурирующую в предложении 54, отождествляя функцию f с функцией $x \mapsto \lfloor x\rfloor^2$ и функцию g с функцией $x \mapsto q_x$, и получим искомый результат.

Следующий этап доказательство требует (это было неизбежно) вычисления пределов и суммы ряда.

(56) Лемма.

В предшествующих обозначениях для натурального числа n имеем

$$\lim_{n\to\infty} \frac{q_n}{n^2} = \sum_{k=1}^{\infty} \mu(k)/k^2.$$

Доказательство.

Ряд, фигурирующий в правой части формулы, является, очевидно, абсолютно сходящимся, так как функция Мёбиуса мажорируется по абсолютной величине единицей. Итак, достаточно оценить разность между общими членами этих двух последовательностей и показать, что она стремится к нулю. Имеем:

$$\sum_{k=1}^{n} \frac{\mu(k)}{k_2} - \frac{q_n}{n^2} = \sum_{k=1}^{n} \mu(k) \times \left(\frac{1}{k^2} - \left\lfloor \frac{n}{k} \right\rfloor^2 \times \frac{1}{n^2}\right).$$

Кроме того, для всякого вещественного положительного числа x имеем $0 \leqslant x - \lfloor x \rfloor < 1$ и, следовательно, $0 \leqslant 1/k - \lfloor n/k \rfloor / n \leqslant 1/n$. В этих условиях

$$0 \leqslant \frac{1}{k^2} - \frac{1}{n^2} \times \lfloor \frac{n}{k} \rfloor^2 = \left(\frac{1}{k} - \frac{1}{n} \times \lfloor \frac{n}{k} \rfloor\right) \times \left(\frac{1}{k} + \frac{1}{n} \times \left[\frac{n}{k}\right]\right) \leqslant \frac{1}{n} \times \frac{2}{k}.$$

Перенося эти значения в разность для мажорирования, получаем:

$$\left(\frac{q_n}{n^2} - \sum_{k=1}^{n} \frac{\mu(k)}{k^2}\right) \leqslant \frac{2}{n} \times \sum_{k=1}^{n} \frac{1}{k} \leqslant \frac{2 \log_n}{n}$$

величина, стремящаяся к нулю, когда n стремится к бесконечно сти. Итак, последовательность $(q_n/n^2)_{n \in \mathbb{N}^\bullet}$. сходится и имеет тот же предел, что и ряд.

Для того, чтобы закончить доказательство теоремы Дирихле, оста ется вычислить сумму ряда с общим членом $\mu(k)/k^2$. Для этого дока жем, что $(\sum_{k=1}^{\infty} \mu(k)/k^2 \times (\sum_{k=1}^{\infty} 1/k^2) = 1$. Оба рассматриваемых ряда — абсолютно сходящиеся, и потому можно изменить порядок суммирования следующим образом:

$$\left(\sum_{k=1}^{\infty} \frac{\mu(k)}{k^2}\right) \times \left(\sum_{m=1}^{\infty} \frac{1}{m^2}\right) = \sum_{k=1}^{\infty} \sum_{m=1}^{k=1} \frac{\mu(k)}{m^2 k^2} = \sum_{d=1}^{\infty} \left(\sum_{k|d} \mu(k)\right) \times \frac{1}{d^2}.$$

По уже доказанному свойству 53 самая внутренняя сумма нулевая, за исключением случая, когда $d = 1$. Сумма ряда с общим членом $1/k^2$ 2 равна $\pi^2/6$. Теорема Дирихле доказана.

Конец этого раздела посвящен классической формуле обращения Мёбиуса.

Рассмотрим множество $\mathbb{N}^*$, упорядоченное с помощью отношения делимости. В этой структуре 1 — наименьший элемент и всякий ин тервал $[a, b]$ конечен. $(\mathbb{N}^*, |)$ — упорядоченное множество, являющееся локально конечным.

Поэтому на множестве функций $\mathcal{F}$, определенных на $\mathbb{N}^*$ со значени ями в A, можно ввести внутренний закон композиции.

(57) Определение

*На $\mathcal{F}$ определен закон внутренней композиции *, называемый арифметическим произведением, по следующему правилу:*

$$\forall f \in \mathcal{F}, \forall g \in \mathcal{F}, \forall n \in \mathbb{N}^*, \quad (f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

(58) Свойства (произведения *)

(i) Произведение ассоциативно и коммутативно.
(ii) Функция Кронекера δ, определяемая как $\delta(1) = 1$ и $\delta(n) = 0$, если $n > 1$, есть нейтральный элемент для произведения $*$.
(iii) Элемент $f \in \mathcal{F}$ обратим для операции $*$ тогда и только тогда, когда $f(1)$ обратим.
(iv) Множество $\mathcal{F}$, наделенное обычным сложением функций и опера цией $*$, является коммутативным унитарным кольцом.

Доказательство (только для пункта (*iii*)).

Пусть $f \in \mathcal{F}$ такой, что $f(1) \in U(A)$. Определим g по индукции следующим образом:

$$g(1) = f(1)^{-1} \quad \text{и} \quad g(n) = -f(1)^{-1} \sum_{hzhz} g(d) f\left(\frac{n}{d}\right) \quad \text{при } n > 1$$

Простая проверка показывает, что g — обратный элемент для f. Остальные утверждения теоремы немедленно выводятся из определения арифметического произведения.

(59) Свойство.

Пусть ξ — элемент из $\mathcal{F}$, определяемый по правилу $\xi(n) = l, \forall n \in \mathbb{N}^*$. Тогда в $(\mathcal{F}, *)$ функции ξ иμ обратны друг другу.

Проблема, решаемая с помощью формулы обращения Мёбиуса, следующая. Пусть g — функция из $\mathbb{N}^*$ в A и пусть f — функция, определенная по правилу $\sum_{d|n} g(g)$ для $n \in \mathbb{N}^*$. Можно ли в этом случае выразить функцию g через f? Другими словами, можно ли найти обращения этой формулы? Ответ дает следующая

(60) Теорема (Формула обращения Мёбиуса).

Пусть f и g — две функции в $\mathcal{F}$, такие, что для любого $n \in \mathbb{N}^*$ справедливо соотношение $f(n) = \sum_{d|n} g(d)$. Тогда можно выразить g через функцию $f : g(n) = \sum_{d|n} \mu(d) f(n/d)$, где μ — функция Мёбиуса.

Доказательство (формулы обращения Мёбиуса).

Выражение f через функцию g описывается в терминах умножения $*: f = \xi * g$, а так как ξ и μ взаимно простые элементы относительно операции * (свойство 59), то получаем $g = \mu * f$.

Более общие сведения по теории арифметических функций можно получить, обратившись к монографии Бержа [19].

1. Расширенный алгоритм Евклида

Этот раздел посвящен изучению эффективного метода получения ко эффициентов Безу в евклидовом и квазиевклидовом кольце. Надо от метить, что квазиевклидовый случай — не единственная возможность для построения таких алгоритмов (известным примером является не евклидово кольцо главных идеалов кольца целых алгебраических чисел в $\mathbb{Q}(\sqrt{-19})$). В следующей главе мы увидим, что наличие коэффициен тов Безу является главным ключом к классификации модулей над коль цом главных идеалов (теория инвариантных множителей): кто умеет их вычислять, тот умеет решать эффективным образом задачи линейной алгебры над кольцом главных идеалов.

1.1. Вычисление коэффициентов Безу в квазиевклидовом кольце

Для квазиевклидова кольца A разновидность алгоритма Евклида, предлож в разделе 3.2, позволяет вычислить коэффициенты Безу. Используемые обозначения те же, что в разделе 3.2. Алгоритм, приме ненный к паре чисел a, b, порождает последовательность $r_{0 \leqslant i \leqslant n+1}$ такую, что

$$r_{i-1} = r_i q_i + r_{i+1} \text{ для } 1 \leqslant i \leqslant n, \text{ где } r_0 = a, r_1 = b, r_{n+1} = 0.$$

Элемент r_{i+1} является линейной комбинацией r_i и $r_{i-1}(r_{i+1} \in Ar_i + Ar_{i-1})$. Так как $r_0 = 1 \cdot a + 0 \cdot b$, $r_1 = 0 \cdot a + 1 \cdot b$, то по предыдущему рекуррентному соотношению для г< получаем, что $r_n = \text{НОД}(a, b)$ — линейная комбинация a и b. Точнее, предполагая, что $r_i = u_i a + v_i b$, получаем:

$$r_{i+1} = r_{i-1} - q_i r_i = (u_{i-1} - q_i u_i)a + (v_{i-1} - q_i v_i)b.$$

Из этих формул легко получается рекуррентная последовательность:

$$hzhzhzhhzh$$

из которой теперь и следует классический результат: $r_n = \text{НОД}(a,b) = u_n a + v_n b$ Эти соотношения приводят, к тому же, к рекуррентному алгоритму, изображенному ниже, в котором тройка (u,v,r) соответ ствует (u_i,v_i,r_i) и тройка (u',v',r') соответствует u_{i+1},v_{i+1},r_{i+1}. Переменная i, бесполезная для алгоритма, присутствует в комментариях только для того, чтобы придать смысл утверждениям.

$$ada\ ada\ ada$$

Вот другое доказательство, основанное на эквивалентном представлении того же алгоритма. Для этого все рекуррентные соотношения (6) запишем в матричной форме:

$$matrix\ matrix$$

Эти равенства дают:

$$matrix\ matrix$$

Затем:

$$matrix\ matrix$$

$matrix\ ada$

Следовательно, для $i = n$ имеем: $a = (-1)^n v_{n+1} r_n,\ \ b = (-1)^{n+1} u_{n+1} r_n$ и $r_n = u_n a + v_n b$. Последние соотношения *явно* показывают, что r_n является, с одной стороны, общим делителем, а с другой — линейной комбинацией a и b. Это порождает новое *эффективное* доказательство, поскольку r_n является НОД a и b. Этот подход позволяет построить самодостаточный алгоритм (3), в котором больше не фигурирует переменная i.

$tabletable$

В таблице 3 приведен пример вычисления коэффициентов Безу в $\mathbb{Z}$. Этот пример может быть полезен для понимания следующего параграфа. В рассматриваемом примере a = 1292, b = 798, их НОД = 38 и найденные коэффициенты Безу u = — 8 и v = 13 (подчеркнутые числа).

Коэффициенты Безу часто применяются для вычисления обратного элемента в $\mathbb{Z}/n\mathbb{Z}$. Пусть, например, требуется обратить класс 34 в $\mathbb{Z}/235\mathbb{Z}$ (34 взаимно просто с 235, следовательно, обратимо по моду лю 235): алгоритм Безу дает соотношение $1 = 11 \times 235 — 76 \times 34$, и обратным к 34 по модулю 235, следовательно, является —76 = 159. Операция обращения часто необходима в модулярной арифметике. Иногда эта конструкция требуется и в других кольцах, например, в кольце целых чисел Гаусса. Так, алгоритм Безу, примененный в $\mathbb{Z}[i]$ к числам $23+14i$ и $7+5i$, дает $1 = (—3+2i)\times(23+14i)+(9—7i)$ и, следовательно, обратным к элементу $7+5i$ по модулю $23+14i$ будет $9—7i$.

1.2. Мажорирование коэффициентов Безу в $\mathbb{Z}$

Равенства $ua+vb = (u-kb)a+(v+ka)b$ и для d, делящего a и b, $ua+vb = (u-kb/d)a+$ показывают, что существует много пар (u, v), для которых НОД$(a, b) = ua+vb$. Расширенный алгоритм Евклида, полученный в предыдущем разделе, позволяет вычислить такую пару (u, v), что, *за исключением лишь некоторых особых случаев,*выполняются неравенства $|u| \leqslant |b/2d|$ и $|v| \leqslant |a/2d|$.

Эти оценки являются объектом исследования для следующего предложения. Единственность такой пары (u, v), удовлетворяющей указанным неравенствам (упр. 33), доказывает, что пара Безу, получаемая алгоритмом Евклида, является самой «красивой».

(61) Предложение.

(i) Пусть a и b — различные строго положительные целые числа, и пусть d их НОД. Пусть $(u_i)_{0\leqslant i\leqslant n+1}$ — последовательности, полученные расширенным алгоритмом Евклида. В этих условиях последовательности $|u_i|_{1\leqslant i\leqslant n+1}$ и $|v_i|_{0\leqslant i\leqslant n+1}$ являются возрастающими, не переполняют разрядную сетку машины — в предположении, что a и b представимы машинными кодами — и указанный алгоритм дает коэффициенты Безу u, v, удовлетворяющие оценкам:

$$|u| \leqslant |b/2d|, \quad |v| \leqslant |a/2d|.$$

(ii) Если (a, b) — пара целых чисел, отличная от $(0, a)$, $(a, 0)$ и $(a, \pm)$, то существуют коэффициенты Безу, удовлетворяющие неравенствам (7)

Доказательство.

Напомним классические обозначения:

$$r_{i-1} = r_i q_i + r_{i+1},\ \ u_{i+1} = u_{i-1} - u_i - u_i q_i,\ \ v_{i+1} = v_{i-1} - v_i q_i, \text{ и } \ u_0 = v_1 = 1,\ \ u_1 = v_0 = 0.$$

Легко убедиться, что $u_{2i} \geqslant 0$ и $u_{2i+1} \leqslant 0$; значит, $|u_{i+1} \geqslant |u_i q_i|$, откуда видно (ввиду $q_i > 0$), что последовательность $(|u_i|)$ возрастающая для $i \geqslant 1$. В конце алгоритма имеем $|u_{n+1}| \geqslant |q_n u_n|$, где $q_n \geqslant 2$, что неверно только для случаев, выписанных в явном виде в (ii). Однако $|u_{n+1}| = a/d$, что заканчивает доказательство (для v_i доказательство аналогично.

2. Факториальность кольца многочленов

Прежде чем закончить эту главу, «пробежимся» по кольцам многочленов, что позволит построить приемлемые алгоритмы вычисления НОД с эффективными оценками трудоемкости. Но сначала немного теории.

(62) Теорема.

(i) Если A — унитарное нётерово коммутативное кольцо, то кольцо многочленов $A[X]$ нётерово. То же верно и для кольца $A[X_1, \dots, X_n]$.
(ii) Если K — поле, то $K[X_1, \dots, X_n]$ нётерово.
(iii) Кольцо многочленов $\mathbb{Z}[X_1, \dots, X_n]$ с целыми коэффициентами нётерово. Для доказательства теоремы нам понадобятся некоторые простые результаты. Пусть n — натуральное число, I — идеал в $A[X]$. Обозначим через $dom_n(I)$ часть A, состоящую из коэффициентов при старших (доминирующих) членах многочленов из I, имеющих степень в точности равную n, и к которой добавлена константа 0.

(63) Лемма.

(i) $dom_n(I)$ — идеал в A.
(ii) Если $n \leqslant m$, то $dom_n(I) \subset dom_m(I)$(рассмотреть $X^{m-n}P$ для в I, имеющего степень n).
(iii) Если $I \subset J$, то $dom_n(I) \subset som_n(J)$.

(64) Лемма.

Пусть $I \subset J$ — два идеала в $A[X]$, такие, что для всякого n: $dom_n(I) = dom_n($
Тогда $I = J$.

Доказательство.

Пусть P — элемент J. Если P степени 0, то очевидно (так как $dom_0(I) = dom_0($ что $P \in I$. В остальных случаях будем использовать индукцию по степени n полинома P. Пусть $P = aX^n + \ldots$ и $a \in dom_n(J) = dom_n(I)$. Поэтому существует $Q \in I$, такой, что $Q = aX^n + \ldots$. Многочлен P—Q имеет степень, меньшую, чем n, и принадлежит J. По предположению индукции получаем —$Q \in I$, а тогда $P \in I$.

Доказательство теоремы 62

Рассмотрим возрастающую последовательность (I_i) идеалов в $A[X]$. Семейство идеалов $(dom_n(I_i))_{i,n}$ имеет максимальный элемент (но не максимум на данный момент) $dom_{n_0}(I_{i_0})$. Следовательно, для всякого $n \geqslant n_0$ и для всякого $i \geqslant i_0$ $dom_n(I_i) = dom_{n_0}(I_{i_0})$. Рассмотрим таблицу:

$$tabletable$$

Существование i_0 и n_0 означает, что столбцы таблицы, ранг которых превышает n_0, стабилизируются, начиная с линии i_0. Более того, стабилизируется всякий столбец с номером $n < n_0$. Поэтому, строки предыдущей таблицы, начиная с некоторого индекса q, совпадают: для всякого $i \geqslant q$ имеем $dom_n(I_i) = dom_n(I_q)$, и по лемме 64 это доказывает, что $I_i = I_q$. Последовательность идеалов в $A[X]$ стабилизируется. Следовательно, $A[X]$ нётерово.

Перейдем теперь к свойствам разложения.

(65) Лемма (гаусса)

Пусть простой элемент p кольца A делит произведение многочленов P и Q над A. Тогда p делит P или Q.

Доказательство.

Пусть p не делит ни P, ни Q. Обозначим через a_i и b_j такие коэффициенты P и Q, соответственно, что i и j — наименьшие номера.

для которых $\nmid a_i$ и $\nmid b_j$. Тогда $\nmid \sum_{k+l=i+j} a_k b_l$, так как p делит все слагаемые этой суммы, кроме первого. Противоречие. В действительности лемма Гаусса не утверждает ничего, кроме того, что «если $/()$ без делителей нуля, то это же утверждение верно и для $A[X]/(p)$».

(66) Определение.

Пусть A — факториальное кольцо. Назовем ***содержанием*** *многочлена P с коэффициентами из A НОД его коэффициентов и обозначим его через $c(P)$. Многочлен P называется* ***примитивным****, если его коэффициенты взаимно просты, т.е. если его содержание равно 1.* ***Примитивная часть*** *P равна $P/c(P)$, это примитивный множитель.*

(68) Следствие.

Пусть P — ***примитивный*** *многочлен с коэффициентами в факториальном кольце A, Q — другой многочлен. Если P делит Q над полем частных кольца A, то он делит Q и в $A[X]$. В частности, если для $a \in A^*$ P делит aQ, то P делит Q*

(69) Теорема (Гаусса)

Пусть A — факториальное кольцо, K — его поле частных, S_a — система представителей неприводимых элементов из A (т.е. такая система, по которой можно единственным образом разложить любой элемент из A). Пусть S' — система представителей неприводимых многочленов в $K[X]$ с коэффициентами из A, являющихся примитивными. Тогда $S' \cup S_A$ — система представителей неприводимых элементов в $A[X]$. В частности, $A[X]$ факториально.

Доказательство.

Пусть $P \in A[X]$ — многочлен положительной степени (в противном случае P раскладывается по системе S_a). В $K[X]$, являющемся кольцом главных идеалов, а следовательно, факториальным, многочлен P можно разложить в произведение неприводимых:

$$P = a \prod_{Q \in S'} Q^{\alpha_Q}, \text{ где } a \in K^* \text{ и } \alpha_Q \in \mathbb{N},$$

a можно записать в виде $a = p/q$, где $p, q \in A$. Следовательно, $qP = p \prod Q^{\alpha_Q}$, что является равенством в $A[X]$. Согласно следствию 68 $\prod Q^{\alpha_Q}$ являющийся примитивным многочленом, делит qP, а потому делит P и $a \in A$ (в силу единственности разложенияв $K[X]$). Но тогда получим разложение в $A[X]$! Разложение в $K[X]$ единственно, так как $K[X]$ факториально. Следовательно, разложение в $A[X]$ единственно.

(70) Следствие.

(i) Если A — факториальное кольцо, то это же верно и для $A[X_1, \ldots, X_n$ и результат, разумеется, верен, если — поле.
(ii) В частности, $\mathbb{Z}[X_1, \ldots, X_n]$ — факториальное кольцо.

Примечания.

1. Теорема Гаусса позволяет охарактеризовать неприводимые элементы в $A[X_1, \ldots, X_n]$. А именно:
   - неприводимые константы в A,
   - неприводимые примитивные многочлены над полем дробей кольца A.

2. Всякое кольцо многочленов над факториальным кольцом факториально. Однако кольцо многочленов над КГИ не является, вообще говоря, КГИ. ($A[X]$ — кольцо главных идеалов тогда и только тогда, когда A — поле).

Идеал $I = (X + 2)\mathbb{Z}[X] + X\mathbb{Z}[X]$ в кольце $\mathbb{Z}[X]$ не является главным, хотя он и максимален, так как это ядро сюръективного морфизма x из $\mathbb{Z}[X]$ на $\mathbb{Z}/2\mathbb{Z}$, который каждому многочлену ставит в соответствие класс четности его постоянного коэффициента. Итак, $\mathbb{Z}[X]/I$ тело, и I — максимальный.

Мы закончим эту, немного абстрактную, часть критерием неприводимости многочлена в факториальном кольце: критерий Эйзенштейна.