МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Нижегородский государственный университет им. Н. И. Лобачевского

М.И. Кузнецов
О.В. Любимцев

Задачи по теории чисел

Учебно-методическое пособие

Рекомендован методической комиссией института ИТММ
для студентов ННГУ, обучающихся по направлению 010301 «Математика»

Нижний Новгород
2019

УДК 512.54
ББК 22.144
К-89

К-89 Кузнецов М.И., Любимцев О.В. ЗАДАЧИ ПО ТЕОРИИ ЧИСЕЛ: Учебно-методическое пособие. – Нижний Новгород: Нижегородский госуниверситет, 2019. – 50 с.

Рецензент: д.ф.-м.н., профессор **Лерман Л.М.**

Предлагаемое учебное пособие содержит необходимые теоретические сведения и набор типовых задач по теории чисел. В основу положены материалы учебников и сборников задач, список которых приведен в конце пособия. Составлено в соответствии с программой курса теории чисел, читаемого для студентов-математиков института информационных технологий, математики и механики.

Пособие издано в рамках развития НИУ «Разработка новых и модернизация существующих образовательных ресурсов».

УДК 512.54
ББК 22.144

Содержание

1. Деление с остатком в евклидовом кольце

Область целостности R называется *евклидовой областью*, если существует какая-либо функция φ из множества его ненулевых элементов во множество $\{0, 1, 2, \dots\}$, обладающая следующим свойством: для любых $a, b \in R$ найдутся такие $q, r \in R$, что $a = bq+r$ и либо $r = 0$, либо $\varphi(r) < \varphi(b)$. Кольца $\mathbb{Z}$, $k[x]$, $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$ являются евклидовыми областями. В $\mathbb{Z}$ в качестве функции φ можно взять обычное абсолютное значение. В кольце $k[x]$ нужному условию будет удовлетворять функция, ставящая в соответствие каждому многочлену его степень. Для $a + bi \in \mathbb{Z}[i]$ можно положить $\varphi(a + bi) = a^2 + b^2$. Элемент q называется (неполным) *частным*, r — *остатком* при делении a на b (обозначение $q = qt(a, b), r = rem(a, b)$). Если $r = 0$, то говорят, что a делится на b (запись $a \vdots b$ или $b|a$).

Примеры решения задач

1. Докажите, что квадрат целого числа не может иметь вид $4k + 2$, $k \in \mathbb{Z}$.

Решение. Рассмотрим произвольное целое число z и поделим его с остатком на 4: $z = 4q + r$, $0 \le r < 4$. Тогда $z^2 = (4q + r)^2 = 4(4q^2 + 2qr) + r^2$. Если $r = 0$ или $r = 2$, то z^2 имеет вид $4k$, $k \in \mathbb{Z}$; если $r = 1$ или $r = 3$, то z^2 имеет вид $4k+1$, $k \in \mathbb{Z}$. Таким образом, квадрат целого числа не может иметь остаток два при делении на 4, то есть не может быть представлен в виде $4k + 2$, $k \in \mathbb{Z}$.

2. В кольце $\mathbb{Z}[i]$ произвести евклидово деление элемента $\alpha = 122+19i$ на элемент $\beta = 5 - 11i$.

Решение.

$$\frac{\alpha}{\beta} = \frac{122 + 19i}{5 - 11i} = \frac{(122 + 19i)(5 + 11i)}{(5 - 11i)(5 + 11i)} = \frac{401}{146} + \frac{1437}{146}i =$$

$$= (3 + 10i) + \left(-\frac{37}{146} - \frac{23}{146}i\right).$$

Отсюда

$$\alpha = \beta(3 + 10i) + (5 - 11i)\left(-\frac{37}{146} - \frac{23}{146}i\right) = \beta(3 + 10i) - 3 + 2i.$$

Итак $\alpha = \beta q + r$, где $q = 3 + 10i$, $r = -3 + 2i$. Здесь $\varphi(r) = 9 + 4 = 13$, $\varphi(\beta) = 25 + 121 = 146$, т.е. $\varphi(r) < \varphi(b)$.

3. При каких натуральных n сократима дробь $\dfrac{8n + 71}{5n + 46}$?

Решение. Пусть числитель $a = 8n + 71$ и знаменатель $b = 5n + 46$ кратны числу d, тогда d делит $5a - 8b = -13$. Отсюда получаем, что если дробь сократима, то только на $d = 13$. Теперь достаточно указать только те значения n, при которых

b (или a) делится на 13. Получаем, что 13 делит $5n + 46$ тогда и только тогда, когда 13 делит число $5n+20$, а это в свою очередь равносильно тому, что 13 делит $n+4$. Таким образом, дробь $\dfrac{8n+71}{5n+46}$ сократима в точности тогда, когда остаток от деления числа n на 13 равен 9.

Замечание. Немного позже запись решения подобных задач мы станем воспроизводить, используя язык и свойства числовых сравнений.

Упражнения

В задачах 1–18 даны некоторые из целых чисел a, b, $qt(a,b)$, $rem(a,b)$. Требуется найти остальные из этих чисел.

№ задач	a	b	$qt(a,b)$	$rem(a,b)$
1.	0	77		
2.	43	15		
3.	-43	15		
4.	-273	35		
5.	-3	-7		
6.	323	17		
7.	-93	-21		
8.		5	7	
9.		3	-2	
10.	25		3	
11.	-30		-4	
12.	1899		73	
13.	-1899		-73	
14.		5		2
15.			5	2
16.	-10			1
17.	-10			2
18.		-21	5	12

19. Может ли при делении целого числа a на целое число $b \neq 0$ получится частное q и некоторый остаток r, если

a) $a = 555$, $q = 19$;

b) $a = 589$, $q = 275$.

20. Найти наибольшее целое число, дающее при делении на 13 частное 17.

21. Доказать, что квадрат нечетного натурального числа при делении на 8 дает остаток 1.

22. Доказать, что сумма квадратов двух последовательных натуральных чисел при делении на 4 дает остаток 1.

23. Доказать, что если каждое из двух чисел при делении на m дает остаток 1, то и их произведение при делении на m дает остаток 1.

24. Доказать, что $3m+2$ не может быть квадратом целого числа.

25. Доказать, что среди пяти последовательных натуральных чисел одно делится на 5.

26. Доказать, что сумма $2n+1$ последовательных натуральных чисел делится на $2n+1$.

27. Докажите, что для любого целого n:

а) n^3-n делится на 3;

б) n^5-n делится на 5.

28. Доказать, что если $7 \mid n^2+k^2$, то $7 \mid n$ и $7 \mid k$.

29. Доказать, что если $m-p \mid mn+pq$, то $m-p \mid mq+np$.

30. При каких целых значениях n следующая дробь есть целое число

а) $\dfrac{4n-7}{2n+3}$;

b) $\dfrac{n^2-n+3}{n+1}$?

31. В кольце $\mathbb{Z}[i]$ произвести евклидово деление

а) 32 на $2+3i$;

b) $-11+13i$ на $3-i$;

c) $15+4i$ на 10;

d) $14+18i$ на $13-19i$.

32. Доказать, что кольцо $\mathbb{Z}[i]$ целых гауссовых чисел является евклидовым кольцом.

33. Доказать, что кольцо $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in Z\}$ является евклидовым (указание: $\varphi(a+b\sqrt{2}) =\mid a^2-2b^2 \mid$).

34. Пусть p — простое число. Обозначим через $\mathbb{Q}_p$ множество всех рациональных чисел, которые можно представить в виде дроби со знаменателем, не делящемся на p. Доказать следующие утверждения:

а) $\mathbb{Q}_p$ — подкольцо кольца рациональных чисел;

b) любой элемент $a \in \mathbb{Q}_p$, $a \neq 0$ можно представить в виде $a = p^k\epsilon$ где $k \in N$, $\epsilon \in \mathbb{Q}_p$.

c) для элемента a из b) положим $\varphi(a) = k$. Тогда Q_p — евклидово кольцо.

35. Доказать, что евклидово кольцо является кольцом главных идеалов.

36. Доказать, что кольцо $\mathbb{Z}[x]$ не является евклидовым (указание: идеал (x,k), где $k \neq 0; \pm1$ не является главным идеалом).

2. Простые и составные элементы факториального кольца

Ненулевой элемент a кольца R называется *составным* (приводимым), если $a = bc$, где ни b, ни c не являются обратимыми. Если из представления $a = bc$ следует, что либо b обратим, либо c обратим, то a называется *простым* (неприводимым). Это определение вполне согласуется с простотой целых чисел или неприводимостью многочленов.

Два элемента области целостности R называются *ассоциированными*, если они отличаются обратимым множителем. Таким образом элементы $a, b \in R$ ассоциированы (обозначение $a \sim b$), если существует такой элемент $c \in U(R)$, что $a = bc$. Нетрудно убедиться в том, что отношение ассоциированности является отношением эквивалентности. Множество всех элементов области целостности распадается на 4 класса:

1) множество, содержащее один элемент — нуль;
2) множество $U(R)$ обратимых элементов;
3) множество составных элементов;
4) множество простых элементов.

Последние два класса могут быть пустыми (если область целостности — поле).

Целостное коммутативное кольцо называется *факториальным* (или кольцом с однозначным разложением на множители), если любой ненулевой необратимый элемент a этого кольца однозначно представим в виде

$$a = p_1 p_2 \dots p_n \tag{1}$$

где $p_1, p_2, \dots p_n$ — простые элементы из R; под однозначностью мы имеем ввиду следующее: если

$$a = q_1 q_2 \dots q_m \tag{2}$$

— другое представление, то $n = m$, и, после подходящей перенумерации элементов, выполнено $p_1 = u_1 q_1$, $p_2 = u_2 q_2, \dots$, $p_n = u_n q_n$, где для любого $i \in \{1, 2, \dots, n\}$ элемент u_i обратим.

Широко известными примерами факториальных колец являются кольцо $\mathbb{Z}$ целых чисел, кольцо $\mathbb{Z}[i]$ целых гауссовых чисел и кольцо $F[x]$ многочленов от одной переменной над полем F. При этом , в случае $\mathbb{Z}$ неприводимые элементы — это простые числа и противоположные к ним; обратимые элементы — это ± 1. Таким образом, в разложениях (1) и (2) числа p и q при подходящей упорядоченности отличаются только знаком. В случае кольца $F[x]$ неприводимые множители отличаются скалярным множителем. Примером нефакториального кольца (но целостного, с разложением на простые множители) является кольцо $\mathbb{Z}[\sqrt{-3}]$ комплексных чисел вида $a + b\sqrt{-3}$, где a и b — целые числа. В этом кольце элемент 4, например, разлагается в произведение неприводимых множителей существенно различными способами:

$$2 \cdot 2 = 4 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

Примеры решения задач

1. Доказать, что наименьший отличный от 1 делитель составного числа a (понятно, что он будет простым) не превосходит $\sqrt{a}$.

<u>Решение</u>.

Действительно, пусть q — этот делитель. Тогда $a = qa_1$ и $a_1 \geq q$. Откуда следует, что $a \geq q^2$ и $q \leq \sqrt{a}$.

2. Доказать, что простое число p кольца $\mathbb{Z}$ является составным элементом кольца $\mathbb{Z}[i]$ тогда и только тогда, когда существуют такие целые числа m, n, что $p = m^2 + n^2$.

<u>Решение</u>.

Необходимость. Пусть простое целое число p является составным элементом в кольце $\mathbb{Z}[i]$. Тогда $p = (a + bi)(c + di)$, где a, b, c, d — целые, $(a + bi)$, $(b + di)$ — необратимые элементы. При этом $|p|^2 = (ac - bd)^2 + (ad + bc)^2$. Поскольку число p — действительное, то оно совпадает с сопряженным ему числом $\overline{p}$, где $\overline{p} = (ac - bd) - (ad + bc)i$. Имеем:

$$p\overline{p} = |p|^2 = a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 = a^2(c^2 + d^2) + b^2(c^2 + d^2) =$$

$$= (c^2 + d^2)(a^2 + b^2) = p^2.$$

Тогда, согласно основной теореме арифметики, получим: $p = a^2 + b^2 = c^2 + d^2$.

Достаточность. Пусть $p = m^2 + n^2$. Тогда $p = (m + ni)(m - ni)$ и элемент p в кольце $\mathbb{Z}[i]$ является составным.

Замечание. Известно, что всякое простое число вида $4k + 1$ всегда представимо в виде суммы двух квадратов целых чисел и такое представление однозначно с точностью до перестановки слагаемых. В тоже время числа вида $4k + 3$ не могут быть представлены в виде суммы $m^2 + n^2$, т.к. сумма $m^2 + n^2$ при делении на 4 дает лишь остатки 0, 1, 2. Таким образом, простыми в $\mathbb{Z}[i]$ являются те и только те простые числа, которые при делении на 4 дают в остатке 3. Полезно также использовать следующий факт. Пусть $p \in \mathbb{Z}[i]$, $p = x + iy$, где $x \neq 0$, $y \neq 0$. Число p является простым элементом кольца $Z[i]$ в точности тогда, когда число $n(p) = x^2 + y^2$, называемое нормой числа p, является простым в кольце $\mathbb{Z}$.

3. Разложить число $18 + 4i$ из кольца $Z[i]$ на простые множители.

<u>Решение</u>.

Заметим, что $18 + 4i = 2(9 + 2i)$. Поскольку, $2 = 1^2 + 1^2$, то число 2 является составным в кольце $Z[i]$, здесь $2 = (1+i)(1-i)$. Норма числа $9+2i$ равна $n(9+2i) = 81+4 = 85$, где $85 = 17 \cdot 5$. Следовательно, число $9+2i$ составное, т.е. $9+2i = \alpha \cdot \beta$, причем $n(\alpha) = 5$, $n(\beta) = 17$. Тогда в качестве α можно, например, взять число $2+i$, а в качестве β — число $4-i$. Получаем искомое разложение на простые множители: $18 + 4i = (1 + i)(1 - i)(2 + i)(4 - i)$.

Упражнения

В задачах 1–13 под объемлющим кольцом понимается кольцо целых чисел.

1. Среди перечисленных чисел указать составные и разложить их на простые множители в кольце $\mathbb{Z}$: 127, 437, 509, 919, 1079.

2. Применив "решето Эратосфена"выписать все простые числа из интервала [2, 100], [190, 200].

3. Доказать, что между n и $n!$ $(n > 2)$ содержится хотя бы одно простое число.

4. Написать 12 последовательных составных чисел. Сколько последовательных составных чисел может встретиться в натуральном ряде?

5. Найти такое натуральное n, что числа n, $n+10$ и $n+14$ — простые.

6. Найти такое простое число p, чтобы $2p^2+1$ тоже было простым.

7. Доказать, что $(3, 5, 7)$ — единственная тройка "простых-близнецов"(два простых числа образуют пару близнецов, если одно из них на 2 больше другого).

8. Найдите все простые числа, которые являются одновременно суммой двух простых чисел и разностью двух простых чисел.

9. Доказать, что при делении простого числа на 30 в остатке не может быть составного числа.

10. Доказать, что если p и $8p^2+1$ — простые, то $8p^2+2p+1$ — тоже простое.

11. Пусть a и n — натуральные числа, большие 1. Докажите, что если число a^n-1 простое, то $a=2$ и n — простое. (Числа вида $q=2^n-1$ называются числами Мерсенна. Например, $2^3-1=7$ и $2^5-1=31$. Неизвестно, бесконечно ли много чисел Мерсенна.)

12. Найти все простые числа вида $\dfrac{n(n+1)}{2}-1$, где n — натуральное число.

13. Докажите, что всякое простое число p, большее трех, представимо в виде $6q \pm 1$, $q \in N$.

14. Является ли число $2^{10}+5^{12}$ составным?

14. Доказать, что отношение ассоциированности является отношением эквивалентности.

15. Найти группу единиц кольца $\mathbb{Z}[i]$.

16. Какие из следующих чисел являются простыми в кольце $\mathbb{Z}[i]$: 5; 7; $2+i$; $1+2i$; $1+3i$; $1-3i$; $3+i$; $3-i$?

17. Найти все разложения на простые множители чисел 2, 5, $9+12i$, $23+7i$, $11+3i$ в кольце $\mathbb{Z}[i]$.

18. Пусть p — простое число в $\mathbb{Z}$. Докажите, что в кольце $\mathbb{Q}_p$ (см. задачу 34 в теме 1) простыми элементами являются p и все ассоциированные с p, и только они.

19. Пусть A — кольцо главных идеалов, $a \in A$, $a \neq 0$. Доказать, что (a) — максимальный идеал тогда и только тогда, когда a — простой элемент кольца A.

20. Пусть A — кольцо главных идеалов, $a \in A$, $a \neq 0$. Доказать, что фактор-кольцо $A/(a)$ является полем в точности тогда, когда a — простой элемент кольца A. Верно ли это утверждение для произвольной области целостности?

3. Наибольший общий делитель и наименьшее общее кратное элементов кольца

Пусть R — целостное кольцо. *Наибольший общий делитель* (или просто НОД) двух элементов $a, b \in R$ есть элемент, обозначаемый символом (a, b) и обладающий двумя свойствами:

1) $d|a, d|b$;

2) $c|a, c|b \Rightarrow c|d$.

Ясно, что вместе с элементом d свойствами 1), 2) обладает любой ассоциированный с ним элемент. Обратно, если c и d — два наибольших общих делителя элементов a и b, то будем иметь $c|d$, $d|c$, так что c и d ассоциированы. Обозначение (a, b) относится к любому из них, т.е. в этой записи ассоциированные элементы не различаются. С учетом этого соглашения к определяющим свойствам 1), 2) наибольшего общего делителя добавятся следующие:

3)$(a, b) = a \Leftrightarrow a|b$;

4)$(a, 0) = a$;

5)$(ta, tb) = t(a, b)$;

6)$((a, b), c) = (a, (b, c))$.

Свойство 6) позволяет распространить понятие на произвольное конечное число элементов.

По аналогии с НОД вводится вводится дуальное понятие *наименьшего общего кратного* $m = [a, b]$ элементов $a, b \in R$, также определенного с точностью до ассоциированности двумя свойствами:

1') $a|m, b|m$;

2') $a|c, b|c \Rightarrow m|c$.

В частности, полагая $c = ab$, получаем, что $m|ab$.

Теорема 3.1. *Пусть для элементов a, b целостного кольца R существуют (a, b) и $[a, b]$. Тогда*

a) $[a, b] = 0 \Leftrightarrow a = 0 \vee b = 0$*;*

b) $\{a \neq 0, b \neq 0, m = [a, b], ab = dm\} \Rightarrow d = (a, b)$.

Из свойств 1), 2), 1'), 2') или теоремы 3.1 нельзя извлечь ни способа вычисления, ни доказательства существования (a, b) и $[a, b]$. В теореме 3.1 в b) устанавливается лишь соотношение между ними.

Теорема 3.2. *Пусть R — область целостности с разложением на простые множители. Однозначность разложения в R (*факториальность *R) имеет место тогда и только тогда, когда любой простой элемент $p \in R$, делящий произведение $ab \in R$, делит по крайней мере один из множителей a, b.*

Пусть R — факториальное кольцо. Обозначим через P такое множество простых элементов в R, что всякий простой элемент из R ассоциирован с одним и только одним элементом из P (такое разбиение возможно, так как отношение ассоциированности является отношением эквивалентности). Рассматривая разложения двух элементов $a, b \in R$ удобно считать, что в них входят одинаковые элементы из P, но некоторые, возможно, с нулевыми показателями, т.е.

$$a = up_1^{k_1} \dots p_s^{k_s}, b = \nu p_1^{l_1} \dots p_s^{l_s}, \tag{$*$}$$

где $u|1$, $\nu|1$; $k_i \geq 0$, $l_i \geq 0$; $p_i \in P$; $1 \leq i \leq r$.

При помощи теоремы 3.2 получается легко запоминаемый

Признак делимости: Пусть a, b — элементы факториального кольца R, записанные в виде (*). Справедливы утверждения:

1) $a|b$ тогда и только тогда, когда $k_i \leq l_i$, $i \in \{1, 2, \dots, s\}$;

2) $(a, b) = p_1^{t_1} \dots p_s^{t_s}$, где $t_i = min\{k_i, l_i\}$, $i \in \{1, 2, \dots, s\}$;

3) $[a, b] = p_1^{h_1} \dots p_s^{h_s}$, где $h_i = max\{k_i, l_i\}$, $i \in \{1, 2, \dots, s\}$;

Таким образом, в качестве t_i нужно брать наименьший из двух показателей , а в качестве h — максимальный. В частности элементы $a, b \in R$ взаимно просты (т.е. $(a, b) = 1$) в точности тогда, когда простые множители, входящие в разложение одного элемента, не входят в разложение другого. Недостаток этого признака делимости заключается в том, что на практике бывает весьма трудно получить разложение вида (*). Даже в случае $R = Z$ приходится довольствоваться незначительными вариациями метода прямого перебора простых чисел, меньших данного числа n. Тем более приятно, что в евклидовых кольцах (которые факториальны) имеется эффективный способ вычисления (a, b) и $[a, b]$. В евклидовых кольцах существует способ нахождения (a, b), называемый *алгоритмом Евклида* и заключающийся в следующем.

Пусть даны ненулевые элементы a, b евклидового кольца R. Применяя достаточно большое (но конечное) число раз алгоритм деления с остатком, мы получим систему равенств с последним нулевым остатком:

$$a = q_1 b + r_1, \varphi(r_1) < \varphi(b)$$

$$b = q_2 r_1 + r_2, \varphi(r_2) < \varphi(r_1)$$

$$r_1 = q_3 r_2 + r_3, \varphi(r_2) < \varphi(r_3)$$

....

$$r_{k-2} = q_k r_{k-1} + r_k, \varphi(r_k) < \varphi(r_{k-1})$$

$$r_{k-1} = q_{k+1} r_k, r_{k+1} = 0$$

Последний отличный от нуля остаток r_k является наибольшим общим делителем элементов a и b.

Теорема 3.3. *В евклидовом кольце R любые два элемента a и b имеют наибольший общий делитель и наименьшее общее кратное. При помощи алгоритма Евклида можно найти такие $u, \nu \in R$, что будет выполнено соотношение $(a, b) = au + b\nu$. В частности, элементы $a, b \in R$ взаимно просты тогда и только тогда, когда существуют элементы $u, \nu \in R$ для которых $au + b\nu = 1$.*

Следствие 3.1. *Пусть a, b, c — элементы евклидового кольца R.*

(i) Если $(a,b)=1$ и $(a,c)=1$, то $(a,bc)=1$.

(ii) Если $a|bc$ и $(a,b)=1$, то $a|c$.

(iii) Если $b|a$, $c|a$ и $(b,c)=1$, то $bc|a$.

Примеры решения задач

1. Найдите наибольший общий делитель и наименьшее общее кратное чисел 1500, -1224, -1440.

Решение. Для решения задачи разложим каждое из чисел 1500, 1224 и 1440 на простые множители. Легко убедиться в том, что $1500 = 2^2\cdot 3^1\cdot 5^3$, $1224 = 2^3\cdot 3^2\cdot 17^1$, $1440 = 2^5\cdot 3^2\cdot 5^1$. Выбирая минимальные значения показателей входящих в разложения простых чисел, мы получим, что $(1500,-1224,-1440) = 2^2\cdot 3^1\cdot 5^0\cdot 17^0 = 2^2\cdot 3 = 12$.

Аналогично, взяв максимальные значения показателей входящих в разложения простых чисел, находим $[1500,-1224,-1440] = 2^5\cdot 3^2\cdot 5^3\cdot 17^1 = 612000$.

2. В кольце $\mathbb{Z}[i]$ вычислить (α,β) и найти линейное представление $d = u\alpha+\nu\beta$, где $\alpha = 14+18i$, $\beta = 13-19i$.

Решение. Разделим евклидово элемент α на β. Получим: $\alpha = \beta q + r$, где $q = i$, $r = -5+5i$; т.к. $r\neq 0$, то делим далее β на r:

$$\frac{\beta}{r} = \frac{13-19i}{-5+5i} = \frac{(13-19i)(-5-5i)}{50} = -\frac{16}{5}+\frac{3}{5}i = (-3+i)+\left(-\frac{1}{5}-\frac{2}{5}i\right).$$

Тогда

$$\beta = (-3+i)(-5+5i)+\left(-\frac{1}{5}-\frac{2}{5}i\right)(-5+5i);$$

т.е. $\beta = (-3+i)r+(3+i)$. Обозначим $3+i$ через r_1. Откуда находим: $\beta = r(-3+i)+r_1$. Т.к. $r_1\neq 0$, то деление продолжаем:

$$\frac{r}{r_1} = \frac{-5+5i}{3+i} = \frac{5(-1+i)(3-i)}{10} = \frac{(-1+i)(3-i)}{2} = -1+2i.$$

Таким образом, $r_2 = 0$, поэтому $d = (14+18i, 13-19i) = r_1 = 3+i$. Для нахождения линейного представления $(\alpha,\beta) = d$ выразим r_1 из равенства $\beta = r(-3+i)+r_1$. Получим: $r_1 = \beta - r(-3+i)$. В свою очередь, r выразим из условия $\alpha = \beta q + r$. Тогда получим, что $d = r_1 = \beta-(-3+i)(\alpha-i\beta) = \alpha(3-i)+\beta(-3i)$. Откуда $d = (3-i)\alpha+(-3i)\beta$, т.е. $u = 3-i$, $\nu = -3i$.

Упражнения

В задачах 1 — 3 а) используя признак делимости и b) с помощью алгоритма Евклида найти:

1. $(607, 477)$.

2. $(343, 246)$.

3. $(6494, 6303)$.

4. Найдите линейное представление наибольших общих делителей в задачах 1 — 3.

5. Найти $(420, 126, 525)$ и $[420, 126, 525]$.

6. Найти $(529, 1541, 1817)$ и $[529, 1541, 1817]$.

7. В кольце $\mathbb{Z}$ привести пример $n \geq 3$ взаимно простых чисел, никакие два из которых не взаимно простые.

8. Найти НОД двух последовательных четных чисел.

9. Найти НОД двух последовательных нечетных чисел.

10. Доказать, что если $(a, b) = 1$, то либо $(a+b, a-b) = 1$, либо $(a+b, a-b) = 2$.

11. Будет ли несократимой дробь $\dfrac{a}{a+b}$, если дробь $\dfrac{a}{b}$ несократима?

12. Пусть $d = (a, b)$, $m = [a, b]$. Найти (d, m); (ab, m); $(a + b, m)$.

13. Пусть $(a, b) = 1$. Найти $(a + b, ab)$.

14. Найти $(n, 2n + 1)$.

15. Найти $(10n + 9, n + 1)$.

16. Найти $(3n + 1, 10n + 3)$.

17. Доказать, что $(a, b) = (5a + 3b, 13a + 8b)$.

18. При любом натуральном n найдите наименьшее общее кратное чисел:

а) $n^3 + 11n$ и 6;

б) $n^5 + 4n$ и 10.

19. Докажите, что $(a, b) \cdot [a, b] = ab$ для любых $a, b \in N$.

20. Найти наименьшее натуральное число, которое кратно числам 2, 3, 4, 5, 6, 7, 8, 9 и 10.

21. Пусть A — кольцо главных идеалов, $a, b \in A$ и $d = (a, b)$. Докажите, что имеет место равенство идеалов $(a, b) = (d)$. Докажите, что для произвольной области целостности это утверждение, вообще говоря, неверно.

22. Пусть A — кольцо главных идеалов. Докажите, что для элементов $a, b \in A$ равенство $A = (a, b)$ выполняется тогда и только тогда, когда $(a, b) = 1$. Верно ли это утвержение для элементов произвольной области целостности?

23. Найти элемент, порождающий идеал (a, b) в $\mathbb{Z}[i]$:

а) $a = 13 + 2i$, $b = -5 - 3i$;

b) $a = 5 + i$, $b = -4 + 7i$;

c) $a = 7 + 2i$, $b = 2 - 7i$.

24. Пусть A — факториальное кольцо, $a, b \in A$, $m = [a, b]$, $d = (a, b)$. Докажите, что ab, md — ассоциированные элементы.

25. Докажите, что в кольце $\mathbb{Z}[i\sqrt{5}]$ числа 2 и $1 + i\sqrt{5}$ являются взаимно простыми.

26. Докажите, что в $\mathbb{Z}[i\sqrt{5}]$ не существует $(2, 1 + i\sqrt{5})$, $(6, 2 + 2i\sqrt{5})$.

4. Важнейшие числовые функции

Функция $\pi(x)$ определяется для всех натуральных x и представляет собой количество простых чисел в натуральном ряду, не превосходящих x. Значение $\pi(x)$ находится точно непосредственным подсчетом простых чисел в натуральном ряду (обычно с использованием таблицы простых чисел) или, при больших значениях , приближенно по формулам:

$$\pi(x) \approx \frac{x}{lnx} \text{ и } \pi(x) \approx \int_2^x \frac{du}{lnu}.$$

Функция $[x]$ определяется для всех вещественных x и представляет собой наибольшее целое число, не превосходящее x. Другими словами, $[x]$ — такое целое число, что $[x] \leq x < [x] + 1$. Эта функция называется *целой частью. Дробной частью* числа x называется число $\{x\} = x - [x]$.

Имеют место следующие утверждения.

1) Пусть $a, b \in \mathbb{Z}$. Тогда $\left[\dfrac{a}{b}\right] = qt(a, b)$.

2) Пусть $a, d \in \mathbb{N}$. Количество натуральных чисел, не превосходящих a и делящихся на d, равно $\left[\dfrac{a}{d}\right]$.

3) Пусть $a, d \in \mathbb{N}$. Тогда $\left[\dfrac{[a]}{d}\right] = \left[\dfrac{a}{d}\right]$.

4) Показатель, с которым простое число p входит в каноническое разложение числа $n!$, равен

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots$$

Рассмотрим функции, определенные на множестве натуральных чисел.

Функцией Мёбиуса называется функция $\mu : \mathbb{N} \to \{-1, 0, 1\}$, определенная условием $\mu(1) = 1$, $\mu(n) = 0$, если n не свободно от квадратов, и $\mu(p_1 p_2 \ldots p_l) = (-1)^l$, где p_i — различные простые числа. Функция Мёбиуса имеет многочисленные применения. В частности, эта функция используется для определения числа неприводимых многочленов данной фиксированной степени в $k[x]$, где k — конечное поле. Например, рассмотрим поле $\mathbb{Z}_p$. В $\mathbb{Z}_p[x]$ имеется конечное число многочленов заданной степени. Пусть $F_d(x)$ — произведение всех приведённых неприводимых многочленов в $\mathbb{Z}_p[x]$ степени d.

Теорема 4.1. $x^{p^n} - x = \prod\limits_{d|n} F_d(x)$.

Пусть N_d — число приведенных неприводимых многочленов степени d в $\mathbb{Z}_p[x]$.

Следствие 4.1. $p^n = \sum\limits_{d|n} dN_d$.

Следствие 4.2. $N_n = n^{-1} \sum_{d|n} \mu \left(\dfrac{n}{d} \right) p^d.$

Следствие 4.3. *Для каждого целого числа $n \geq 1$ в $\mathbb{Z}_p[x]$ существует неприводимый многочлен степени n.*

Функцией Эйлера $\varphi(a)$ называется функция $\varphi : \mathbb{N} \to \mathbb{N}$, где $\varphi(a)$ — количество натуральных чисел, не превосходящих и взаимно простых с a.

Функция $\Theta : \mathbb{N} \to \mathbb{N}$ называется *мультипликативной*, если $\Theta \neq 0$ и из $(a, b) = 1$ следует $\Theta(ab) = \Theta(a)\Theta(b)$, и называется *вполне мультипликативной*, если $\Theta \neq 0$ и $\Theta(ab) = \Theta(a)\Theta(b)$ для любых a, b.

Известно, что функции Мёбиуса и Эйлера мультипликативны. Также являются мультипликативными функции $\tau(a)$ и $s(a)$, где $\tau(a)$ — количество натуральных делителей натурального числа, $s(a)$ — их сумма.

Теорема 4.2. *Пусть $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ — каноническое разложение числа n и Θ — мультипликативная функция. Тогда*

$$\sum_{d|n} \Theta(d) = (1 + \Theta(p_1) + \ldots + \Theta(p_1^{\alpha_1})) \cdot \ldots \cdot (1 + \Theta(p_k) + \ldots \Theta(p_k^{\alpha_k}))$$

(Здесь в левой части стоит сумма значений функции по всем делителям числа)

Теорема 4.3. *Если Θ — мультипликативная функция, то и функция $\psi(n) = \sum_{d|n} \Theta(d)$ — тоже мультипликативная функция.*

Теорема 4.4 (Гаусс)**.**

$$\sum_{d|n} \varphi(d) = n.$$

Теорема 4.5. *Пусть $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ — каноническое разложение числа n. Тогда*

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_k}\right).$$

Примеры решения задач

1. Решите уравнение $[x] = 1 + 2\{x\}$.

Решение. Достаточно заметить, что число $1 + 2\{x\}$ обязано быть целым и, следовательно, $\{x\} = 0$ или $\{x\} = 0,5$. В первом случае $[x] = 1$, то есть $x = [x] + \{x\} = 1 + 0 = 1$. Во втором случае $[x] = 2$, то есть $x = [x] + \{x\} = 2 + 0,5 = 2,5$. Таким образом, решениями уравнения $[x] = 1 + 2\{x\}$ являются числа 1 и 2,5.

2. Решите уравнение $\varphi(x) = 2$.

Решение. Очевидно, что $x \neq 1$. Имеем:

$$x = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, \quad \varphi(x) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \dots p_k^{\alpha_k - 1}(p_1 - 1) \dots (p_k - 1).$$

Пусть $\varphi(x) = 2^m l$, где l нечетно. Поскольку для нечетного простого числа p величина $p-1$ четна, то в каноническом разложении x имеется не более m нечетных простых множителей. Другими словами, $k \leq m+1$, причем если $k = m+1$, то $p_1 = 2$. В нашем случае $m = 1$, то есть $k \leq 2$, причем если $k = 2$, то $p_1 = 2$.

Пусть $k = 1$, то есть $x = p^\alpha$. Если $p = 2$, то $\varphi(x) = \varphi(2^\alpha) = 2^{\alpha-1}$, и наше уравнение принимает вид $2^{\alpha-1} = 2$, откуда следует, что $\alpha = 2$ и $x = 2^2 = 4$. Если $p \neq 2$, то $\varphi(x) = \varphi(p^\alpha) = p^{\alpha-1}(p-1)$, и наше уравнение принимает вид $p^{\alpha-1}(p-1) = 2$, откуда следует, что $p - 1 = 2$ и $p^{\alpha-1} = 1$. Таким образом, $p = 3$, $\alpha = 1$ и $x = 3$.

Пусть $k = 2$, то есть $x = 2^\alpha p^\beta$. Тогда $\varphi(x) = \varphi(2^\alpha p^\beta) = 2^{\alpha-1}p^{\beta-1}(p-1)$, и наше уравнение принимает вид $2^{\alpha-1}p^{\beta-1}(p-1) = 2$, откуда следует, что $p - 1 = 2$, $2^{\alpha-1} = 1$ и $p^{\beta-1} = 1$. Таким образом, $p = 3$, $\alpha = \beta = 1$, и $x = 2 \cdot 3 = 6$. Итак, решения уравнения $\varphi(x) = 2$ — это натуральные числа 3, 4 и 6.

3. Найти число неприводимых многочленов на полем $\mathbb{Z}_2$ степеней 2, 3, 4, 5.

Решение. Для $n = 2$, применив формулу следствия 4.2, имеем:

$N_1 = 2$, $N_2 = \dfrac{1}{2}(2^2 - 2) = 1$, $N_3 = \dfrac{1}{3}(2^3 - 2) = 2$, $N_4 = \dfrac{1}{4}(2^4 - 2^2) = 3$, $N_5 = \dfrac{1}{5}(2^5 - 2) = 6$.

Упражнения

1. Найти точные значения $\pi(10)$, $\pi(25)$, $\pi(50)$.

2. Найти целые и дробные части следующих чисел: 1) 3,14; 2) -3,14; 3) π; 4) -3; 5) 5; 6) $2 + \sqrt[3]{987}$; 7) $\dfrac{7 - \sqrt{21}}{2}$; 8) $\dfrac{10}{3 + \sqrt{3}}$; 9) 0; 10) $1,33 + 2tg\,\dfrac{\pi}{4}$; 11) $log_2 5$; 12) $sin\,1^0$; 13) $sin\,1$; 14) $-e$.

3. Построить графики функций $y = [x]$ и $y = \{x\}$.

4. Выразить $[x + y]$ через целые и дробные части чисел x и y.

5. Сколько натуральных чисел, меньших 1000, не делятся ни на 5, ни на 7?

6. Найти количество натуральных чисел, не превосходящих 100 и взаимно простых с 36.

7. С каким показателем степени число 7 входит в каноническое разложение числа 100! ?

8. Найти каноническое разложение числа 11!

9. С каким показателем степени простое число p входит в каноническое разложение числа $(p^n)!$?

10. Решите уравнения а) $[2x] = 2$; б) $[x] + 5 = \{x\}$.

11. Найти множество значений функции $y = [x] - 2\left[\dfrac{x}{2}\right]$.

12. Докажите формулу Эрмита:

$$[x] + \left[x + \frac{1}{n}\right] + \left[x + \frac{2}{n}\right] + \ldots + \left[x + \frac{n-1}{n}\right] = [nx],$$

где $n \in \mathbb{N}$.

13. Составить таблицу значений функции Мёбиуса для $1 \leq a \leq 20$.

14. Вычислить $\mu(61)$, $\mu(100)$, $\mu(997)$, $\mu(1000)$.

15. Доказать мультипликативность функции Мёбиуса.

16. Являются ли мультипликативными (вполне мультипликативными) функции $f(n) = \sin n$, $f(n) = \dfrac{1}{n^2}$, $f(n) = n^\alpha$, $f(n) = n^2$?

17. Докажите, что мультипликативной является функция Лиувилля $l(n)$, определяемая как $l(n) = (-1)^{\omega(n)}$, где $\omega(n)$ — число простых делителей n, считаемых с повторениями. Является ли она вполне мультипликативной?

18. Вычислить $\varphi(61)$, $\varphi(100)$, $\varphi(997)$, $\varphi(1000)$, $\varphi(125)$, $\varphi(360)$.

19. Доказать, что $\varphi(n^\alpha) = n^{\alpha-1}\varphi(n)$.

20. Доказать, что $\varphi(4n) = 2\varphi(n)$, если $(n, 2) = 1$, и $\varphi(4n) = 2\varphi(2n)$ если $(n, 2) = 2$.

Пусть $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ — каноническое разложение числа $n \in \mathbb{N}$.

21. Доказать, что $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdot \ldots \cdot (\alpha_k + 1)$.

22. Вывести формулу для вычисления $s(n)$ по заданному каноническому разложению числа n.

23. Вычислить: 1) $\tau(61)$; 2) $\tau(100)$; 3) $\tau(997)$; 4) $\tau(125)$.

24. Вычислить: 1) $s(61)$; 2) $s(100)$; 3) $s(1257)$; 4) $s(4000)$.

25. Пусть $N = p^\alpha q^\beta$, где $p \neq q$ — простые числа. N^2 имеет 15 различных делителей. Сколько различных делителей имеет N^3?

26. Определим функцию $s_2(n)$ как сумму квадратов всех натуральных делителей натурального числа $n : s_2(n) = \sum\limits_{d|n} d^2$. Докажите формулу

$$s_2(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}) = \frac{p_1^{2(\alpha_1+1)}}{p_1 - 1} \cdot \frac{p_2^{2(\alpha_2+1)}}{p_2 - 1} \cdot \ldots \cdot \frac{p_k^{2(\alpha_k+1)}}{p_k - 1}.$$

27. Доказать бесконечность множества простых чисел с помощью функции Эйлера (Указание. Предположив, что множество простых чисел конечно и состоит из чисел p_1, p_2,..., p_s, рассмотреть их произведение).

28. *Произведением Дирихле* функций $f(n)$ и $g(n)$ называется функция

$$f \circ g(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

Введем функции $E(n) = 1 \; \forall \; n$, $I(n) = n \; \forall \; n$, а также

$$J(n) = \begin{cases} 1, & \text{если } n = 1; \\ 0, & \text{если } n > 1. \end{cases}$$

Доказать, что

1) $J \circ f = f$ для любой функции $f(n)$;

2) $E \circ E = \tau$;

3) $I \circ E = s$;

4) $I \circ I(n) = n\tau(n)$;

5) $\mu \circ E = J$.

29. Доказать равенства:

1) $\mu \circ \tau = \mu \circ E \circ E = J \circ E = E$;

2) $\mu \circ s = \mu \circ E \circ I = J \circ I = I$.

30. Доказать, что из мультипликативности функций $f(n)$ и $g(n)$ следует мультипликативность функции $f \circ g(n)$.

31. Проверить, что для функции $f'(n)$, определяемой соотношениями

$$f'(1) = 1; f'(p) = -f(p);$$
$$f'(p^n) = -\left(f(p^n) + f(p^{n-1})f'(p) + \ldots + f(p)f'(p^{n-1})\right),$$

выполнено $f \circ f' = J$.

32. Доказать, что мультипликативные функции образуют абелеву группу с единицей J и произведением Дирихле в качестве групповой операции.

33. Найти число неприводимых многочленов на полем $\mathbb{Z}_3$ степеней 2, 3, 4, 5.

34. Пусть p и q — различные нечетные простые числа. Показать, что число приведенных неприводимых многочленов степени q в $\mathbb{Z}_p$ равно $q^{-1}(p^q - p)$.

5. Цепные дроби

Выражение вида

$$\beta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\dots a_{n-1} + \cfrac{1}{a_n}}}}$$

где $a_i \in \mathbb{Z}$, $a_1, a_2, \dots, a_{n-1} \geq 1$, причём $a_n > 1$, называется *конечной цепной дробью.* Числа a_i называются *неполными частными*, n — *длиной* цепной дроби. Цепная дробь, как числовое выражение, равна некоторому рациональному числу, которое называется *значением дроби.* Неполные частные однозначно определяют цепную дробь, поэтому для записи цепной дроби часто используют сокращённую форму записи:

$$\beta = [a_0, a_1, a_2, \dots, a_n].$$

Для каждой цепной дроби можно рассматривать подходящие дроби. А именно, *k-той подходящей дробью*($k \leq n$) к данной цепной дроби называется число (цепная дробь)

$$A_k = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\dots a_{k-1} + \cfrac{1}{a_k}}}}$$

Бесконечная цепная дробь – это выражение вида:

$$A_k = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\dots a_k + \cfrac{1}{\dots}}}}$$

где все a_i — целые числа, причём $a_i \geq 1$ начиная с $i = 1$. *Значением бесконечной цепной дроби* по определению полагается $\lim\limits_{k\to\infty} A_k$. Многие свойства являются общими для конечных и бесконечных цепных дробей, поэтому в дальнейшем, если не оговорено противное, рассматриваются сразу оба случая.

Определим числа P_k и Q_k по индукции при помощи следующих соотношений:

$$P_0 = a_0, P_1 = a_0a_1 + 1, P_k = P_{k-1}a_k + P_{k-2}, k \geq 2;$$

$$Q_0 = 1, Q_1 = a_1, Q_k = Q_{k-1}a_k + Q_{k-2}, k \geq 2.$$

Теорема 5.1 (свойства подходящих дробей)**.** *Пусть дана цепная дробь* $[a_0, a_1, a_k, \ldots]$ *, тогда имеют место следующие свойства.*

1) $A_k = \dfrac{P_k}{Q_k}$.

2) $P_k Q_{k-1} - P_{k-1} Q_k = (-1)^{k-1}$.

3) $(P_k, Q_k) = 1$.

4) $\dfrac{P_k}{Q_k} - \dfrac{P_{k-1}}{Q_{k-1}} = \dfrac{(-1)^{k-1}}{Q_k Q_{k-1}}$,

5) Числа Q_i *образуют монотонно возрастающую последовательность:*

$$1 = Q_0 \leq Q_1 < Q_2 < Q_3 < \ldots.$$

6) $P_k Q_{k-2} - P_{k-2} Q_k = (-1)^k a_k$.

7) Чётные подходящие дроби образуют возрастающую последовательность, нечётные подходящие дроби образуют убывающую последовательность. Всякая чётная подходящая дробь меньше любой нечётной.

8) Модуль расстояния между соседними подходящими дробями монотонно уменьшается и стремится к 0, если дробь бесконечна.

Теорема 5.2. *Всякое рациональное число представимо в виде конечной цепной дроби, причём такое представление единственно. Неполные частные цепной дроби равны частным в алгоритме Евклида. Длина цепной дроби равна длине алгоритма Евклида.*

Бесконечные цепные дроби являются достаточно удобным и точным инструментом для приближённого представления чисел.

Пусть $\beta = [a_0, a_1, a_2, \ldots]$ – цепная дробь (конечная или бесконечная). Полными частными этой дроби называются числа β_0, β_1, β_2, ..., которые определяются соотношениями

$$\beta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ldots a_{k-1} + \cfrac{1}{\beta_k}}}}, \qquad k > 0, \quad \beta_0 = \beta.$$

Данные числа определены однозначно, т.к. они однозначно выражаются через числа β, a_0, a_1,..., a_{k-1}. Для конечных цепных дробей очевидно, что

$$\beta_k = [a_k, a_{k+1}, \ldots, a_n] = a_k + \cfrac{1}{a_{k+1} + \cfrac{1}{\ldots a_{n-1} + \cfrac{1}{a_n}}}, \qquad k \leq n,$$

т.е. k-тое полное частное – это часть цепной дроби, начиная с a_k .

Теорема 5.3. *Пусть $\beta = [a_0, a_1, a_2, \ldots]$ — цепная дробь и b_{k+1} — полное частное, тогда выполняются следующие равенства.*

1) $\beta = \dfrac{P_k\beta_{k+1} + P_{k-1}}{Q_k\beta_{k+1} + Q_{k-1}}$, $k \geq 1$;

2) $\beta_k = [a_k, a_{k+1}, a_{k+2}, \ldots]$;

3) $a_k = [\beta_k]$.

Если бесконечная цепная дробь является периодической, то её значение можно найти, используя свойства полных частных. Кроме того, это значение можно найти, воспользовавшись периодичностью (см. пример 2).

Теорема 5.4. *Всякое действительное число единственным образом представимо в виде цепной дроби. Если число рациональное, то дробь конечная. Если число иррациональное, то дробь бесконечная.*

Алгоритм разложения в цепную дробь состоит в следующем. Полагаем $a_0 = [\beta]$ и рассматриваем число $x_1 = \dfrac{1}{\beta - a_0} \Rightarrow \beta = a_0 + \dfrac{1}{x_1}$. Согласно определению $\beta_1 = x_1$. Далее продолжаем аналогично.

$$a_1 = [\beta_1], \quad x_2 = \frac{1}{\beta_1 - a_1} \quad \Rightarrow \beta_1 = a_1 + \frac{1}{x_2} \quad \Rightarrow$$

$$\Rightarrow \beta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{x_2}} \quad \Rightarrow \beta_2 = x_2;$$

$$a_2 = [\beta_2], \quad x_3 = \frac{1}{\beta_2 - a_2} \quad \Rightarrow \quad \ldots.$$

Каждый шаг алгоритма состоит из двух действий.

1) Нахождение k-го неполного частного как целой части соответствующего полного частного: $\beta_k = [a_k]$.

2) Нахождение следующего полного частного по формуле

$$\beta_{k+1} = \frac{1}{\beta_k - a_k}.$$

На каждом шаге алгоритма получается равенство вида

$$\beta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ldots a_k + \cfrac{1}{\beta_{k+1}}}}} = [a_0, a_1, a_2, \ldots, a_k, \beta_{k+1}].$$

Оно даёт начальную часть разложения числа β в цепную дробь. Если число β является иррациональным, то процесс разложения продолжается бесконечно (см. пример 3).

Теорема 5.5 (Лагранж). *Число β представимо в виде периодической цепной дроби тогда и только тогда, когда β — квадратичная иррациональность (т.е. иррациональный корень некоторого квадратного уравнения с целыми коэффициентами).*

Пусть β равно значению цепной дроби $[a_0, a_1, a_2, \ldots]$. Для достаточно больших значений k дробь $\dfrac{P_k}{Q_k}$ можно считать приближённым значением числа β. В доказательстве теоремы о существовании значения дроби получена *оценка точности этого приближения*:

$$\left|\beta - \frac{P_k}{Q_k}\right| < \frac{1}{Q_k^2}, \qquad \text{т.е.} \quad \beta = \lim_{n\to\infty} \frac{P_k}{Q_k}.$$

С помощью цепных дробей можно решать неопределенные уравнения, в частности, *уравнение Пелля* $x^2 - Dy^2 = \pm 1$, где D - натуральное число, не являющееся полным квадратом. Для решения уравнения $x^2 - Dy^2 = \pm 1$ разложим число $\sqrt{D}$ в цепную дробь. Известно, что данное разложение имеет вид

$$\sqrt{D} = [a_0, (a_1, a_2, \ldots, a_{k-1}, 2a_0)],$$

то есть полученная цепная дробь является периодической. Пусть k — длина периода указанной цепной дроби. Нетрудно доказать, что все натуральные решения уравнения $x^2 - Dy^2 = 1$ могут быть найдены по формулам $x = P_{kn-1}$, $= Q_{kn-1}$, где $n \in \mathbb{N}$, причем kn — четно. Другими словами, уравнение $x^2 - Dy^2 = 1$ имеет бесконечно много решений. Аналогично, все натуральные решения уравнения $x^2 - Dy^2 = -1$ могут быть найдены по формулам $x = P_{kn-1}$, $y = Q_{kn-1}$, где $n \in \mathbb{N}$, причем kn — нечетно. В этом случае $x^2 - Dy^2 = -1$ уравнение не имеет решений при четном k.

Примеры решения задач

1. Представить в виде цепной дроби число $\beta = \dfrac{18}{7}$.
Решение.

$$18 = 7 \cdot 2 + 4,$$
$$7 = 4 \cdot 1 + 3,$$
$$4 = 3 \cdot 1 + 1,$$
$$3 = 1 \cdot 3.$$

Таким образом,

$$\frac{18}{7} = [2, 1, 1, 3] = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3}}}.$$

Используя рекуррентные соотношения из определения подходящих дробей, можно достаточно быстро вычислять все подходящие дроби. По определению $P_0 = a_0$, $Q_0 = 1$. Если формально ввести $P_{-1} = 1$, $Q_{-1} = 0$, то вычисление P_n и Q_n можно оформить в виде таблицы

	a_0	a_1	a_2	$\dots$	a_n
1	a_0	P_1	P_2	$\dots$	P_n
0	1	Q_1	Q_2	$\dots$	Q_n

Для получения P_k надо число в последней заполненной клетке P_{k-1} умножить на a_k и прибавить содержимое предпоследней клетки P_{k-2}. Строка знаменателей подходящих дробей заполняется аналогично. Для приведенного примера получим:

	2	1	1	3
1	2	3	5	18
0	1	1	2	7

В результате вычислены все дроби, подходящие к данной цепной дроби:

$$A_0 = \frac{2}{1} = 2, A_1 = \frac{3}{1} = 3, A_2 = \frac{5}{2}, A_3 = \frac{18}{7}.$$

Последняя подходящая дробь, естественно, совпадает с исходным числом. Если подходящие дроби не нужны, то можно использовать упрощенную схему вычислений: последовательность элементов цепной дроби записываем в обратном порядке, а дальше проводим вычисления по прежней схеме. Значение дроби равно отношению последней скобки к предпоследней:

	3	1	1	2
1	3	4	7	18

2. Найти $\beta = [3, 1, 2, 1, 2, 1, 2, \dots]$.

Решение. Рассмотрим первое полное частное, которое является чисто периодическим $\alpha = \beta_1 = [1, 2, 1, 2, 1, \dots]$. Для него выполняется равенство

$$\beta = 3 + \frac{1}{\alpha}.$$

Воспользовавшись периодичностью α, получаем

$$\alpha = 1 + \cfrac{1}{2 + \cfrac{1}{\alpha}}.$$

Число α легко находится из этого условия:

$$\alpha = 1 + \cfrac{1}{2 + \cfrac{1}{\alpha}} = 1 + \frac{\alpha}{2\alpha + 1} = \frac{3\alpha + 1}{2\alpha + 1} \Leftrightarrow 2\alpha^2 + \alpha = 3\alpha + 1 \Leftrightarrow$$

$$\Leftrightarrow 2\alpha^2 - 2\alpha - 1 = 0 \Leftrightarrow \alpha = \frac{1 \pm \sqrt{3}}{2}$$

Отрицательное значение не подходит, т.к. по определению $\alpha > 0$, поэтому $\alpha = \dfrac{1+\sqrt{3}}{2}$.

Подставляем это число в первую формулу и находим

$$\beta = 3 + \frac{1}{\alpha} = 3 + \frac{2}{1+\sqrt{3}} = \frac{5+3\sqrt{3}}{1+\sqrt{3}} = \frac{(5+3\sqrt{3})(1-\sqrt{3})}{(1+\sqrt{3})(1-\sqrt{3})} = 2+\sqrt{3}.$$

3. Разложить в цепную дробь число $\beta = 2+\sqrt{3}$.

Решение. Применяем алгоритм.

1-Й ШАГ.

$$a_0 = [\beta] = [2+\sqrt{3}] = 3,$$

$$\beta_1 = \frac{1}{\beta - a_0} = \frac{1}{(2+\sqrt{3})-3} = \frac{\sqrt{3}+1}{(\sqrt{3}-1)(\sqrt{3}+1)} = \frac{\sqrt{3}+1}{2}.$$

2-Й ШАГ.

$$a_1 = [\beta_1] = \left[\frac{\sqrt{3}+1}{2}\right] = 1,$$

$$\beta_2 = \frac{1}{\beta_1 - a_1} = \frac{1}{\dfrac{\sqrt{3}+1}{2} - 1} = \frac{2}{\sqrt{3}-1} = \frac{2(\sqrt{3}+1)}{(\sqrt{3}-1)(\sqrt{3}+1)} = \sqrt{3}+1.$$

3-Й ШАГ.

$$a_2 = [\beta_2] = [\sqrt{3}+1] = 2,$$

$$\beta_3 = \frac{1}{\beta_2 - a_2} = \frac{1}{\sqrt{3}+1-2} = \frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{(\sqrt{3}-1)(\sqrt{3}+1)} = \frac{\sqrt{3}+1}{2}.$$

Полное частное повторилось: $\beta_1 = \beta_3$, поэтому дальше и полные и неполные частные будут повторяться с периодом 2:

$$1 = a_1 = a_3 = a_5 = \ldots,$$

$$2 = a_2 = a_4 = a_6 = \ldots.$$

В результате $2+\sqrt{3} = [3, 1, 2, 1, 2, \ldots]$, как было заранее известно из предыдущего примера.

4. Найти первые четыре элемента в разложении $\beta = \sqrt[3]{2}$ в цепную дробь.

Решение. Имеем:

$$\beta^3 - 2 = 0. \qquad (1)$$

Далее, $a_0 = [\beta] = 1$. Следовательно,

$$\beta = 1 + \frac{1}{\beta_1}.$$

Подставив это выражение в (1), получим уравнение для β_1:

$$\frac{1}{\beta_1^3} + \frac{3}{\beta_1^2} + \frac{3}{\beta_1} - 1 = 0.$$

Умножив на β_1^3 и сменив знак, приходим к уравнению

$$\beta_1^3 - 3\beta_1^2 - 3\beta_1 - 1 = 0. \tag{2}$$

Легко видеть, что положительный корень уравнения (2) лежит между 3 и 4 (он единственный, так как уравнение (1) имеет единственный положительный корень), т.е. $a_1 = [\beta_1] = 3$, и

$$\beta_1 = 3 + \frac{1}{\beta_2}.$$

Подставим это выражение в (2) и, после преобразований получим уравнение для β_2:

$$10\beta_2^3 - 6\beta_2^2 - 6\beta_2 - 1 = 0, \tag{3}$$

Положительный корень этого уравнения лежит между 1 и 2, т.е.

$$\beta_2 = 1 + \frac{1}{\beta_3}, a_2 = [\beta_2] = 1.$$

Подставим выражение для β_2 в (3) и придем к уравнению для β_3:

$$3\beta_3^3 - 12\beta_3^2 - 24\beta_3 - 10 = 0,$$

Положительный корень этого уравнения лежит между 5 и 6, т.е. $a_3 = [\beta_3] = 5$. Итак,

$$\sqrt[3]{2} =< 1, 3, 1, 5, \ldots > .$$

Вычислим подходящие дроби

		1	3	1	5
P	1	1	4	5	29
Q	0	1	3	4	23

Таким образом, $\sqrt[3]{2} \approx \frac{29}{23}$, причем ошибка не превосходит $\frac{1}{23^2} = \frac{1}{529}$.

Упражнения

1. Разложить следующие рациональные числа в цепные дроби:

$$1)\frac{127}{52};\quad 2)\frac{24}{35};\quad 3)1,23;\quad 4)\frac{95122}{53808};\quad 5)2,3547;\quad 6)\frac{99}{170}.$$

2. Свернуть непрерывные дроби:

$$1) < 1,1,2,1,2,1,2 >; \qquad 2) < 0,1,2,3,4,5 >;$$

$$3) < 5,4,3,2,1 >;\quad 4) < a,a,a,a,a >;\quad 5) < a,b,a,b,a > .$$

3. Решить уравнения:

$$1) < x,2,3,4 >= \frac{73}{30};\quad 2) < 2,x,3,4 >= \frac{73}{30};$$

$$3) < 2,3,x,4 >= \frac{73}{30};\quad 4) < 2,3,4,x >= \frac{73}{30}.$$

Как было отмечено, при любом $k \geq 1$ $(P_k, Q_k) = 1$, т.е. все подходящие дроби несократимы. Это дает возможность сокращать дроби.

4. При помощи цепных дробей сократить дроби:

$$1)\frac{3587}{2743};\qquad 2)\frac{1043}{3427};\qquad 3)\frac{1491}{2247}.$$

5. Следующие числа заменить подходящими дробями с возможно меньшими знаменателями так, чтобы погрешность не превосходила 10^{-4}:

$$1)\frac{1261}{881};\qquad 2)\frac{587}{103};\qquad 3)3,14159.$$

6. Разложить в периодические цепные дроби и вычислить с точностью до 10^{-4} следующие квадратичные иррациональности:

$$1)\sqrt{5};\quad 2)\sqrt{13};\quad 3)\sqrt{42};\qquad 4)\sqrt{59};\quad 5)\frac{\sqrt{5}-1}{2};$$

$$6)\frac{2-\sqrt{3}}{5};\qquad 7)\frac{5+\sqrt{2}}{2}.$$

7. Найти квадратичную иррациональность, которая разлагается в следующую цепную дробь:

$$1) < (2,3) >;\quad 2) < (1,1,2,2) >;\quad 3) < (3,4,5,2,1) >;$$

$$4)<1,2,3,(4)>; \qquad 5)<a,a,(2a)>;$$

$$6)<0,1,1,1,1,(2)>; \quad 7)<2,1,2,(1,1,3)>; \quad 8)<4,(1,1,2,1,1,8)>.$$

8. Найти 5 первых элементов в разложении следующих чисел в цепную дробь. Оценить погрешность, которая получается при замене данного числа подходящей дробью: 1) $\sqrt[3]{6}$; 2) $\sqrt[3]{3}$; 3) наибольший положительный корень уравнения $x^3 - x^2 - 2x + 1 = 0$; 4) положительный корень уравнения $x^4 - x - 1 = 0$.

9. Найти три первых элемента в разложении $\log_2 5$ в цепную дробь.

10. Найти первые пять подходящих дробей в разложении в цепную дробь числа

$$\pi = 3,1415926535897\ldots$$

11. Найти первые пять подходящих дробей в разложении в цепную дробь числа

$$e = 2,71828182845904\ldots$$

12. Является ли $\delta = -\dfrac{39}{16}$ подходящей дробью к $\alpha = \dfrac{\sqrt{17}-9}{2}$? Если да, оцените точность приближения α числом δ. Какое из неравенств верно: $\alpha > \delta$ или $\alpha < \delta$?

13. Является ли $\delta = -\dfrac{13}{7}$ подходящей дробью к $\alpha = \dfrac{\sqrt{10}-4}{2}$ с точностью 10^{-2}? Какое из неравенств верно: $\alpha > \delta$ или $\alpha < \delta$?

12. Укажите первые четыре натуральных решения уравнения

$$a) x^2 - 3y^2 = 1; \qquad x^2 - 3y^2 = -1;$$

$$b) x^2 - 5y^2 = 1; \qquad x^2 - 5y^2 = -1.$$

13. Укажите наименьшее натуральное решение уравнения:

$$a) x^2 - 41y^2 = 1; \qquad x^2 - 41y^2 = -1;$$

$$b) x^2 - 13y^2 = 1; \qquad x^2 - 13y^2 = -1.$$

6. Отношение сравнимости. Классы вычетов

Два целых числа a и b называются *сравнимыми по модулю* n, $n \in \mathbb{N}$, если a и b имеют одинаковые остатки при делении на n, или, что то же, если $n|(a-b)$. В этом случае пишут $a \equiv b\,(mod\,n)$ или коротко $a \equiv b\,(n)$.

Свойства отношения сравнимости:

1. Отношение сравнимости $\equiv$ является отношением эквивалентности;

2. Если $a \equiv b\,(mod\,n)$, то $f(a) \equiv f(b)\,(mod\,n)$ для любого многочлена $f(x)$ с целыми коэффициентами;

3. $a \equiv b\,(mod\,n) \Leftrightarrow ka \equiv kb\,(mod\,kn)$, где $k \in \mathbb{N}$;

4. $a \equiv b\,(mod\,n) \Leftrightarrow ka \equiv kb\,(mod\,n)$, где $k \in \mathbb{Z}$, $(k,n)=1$;

5.
$$\begin{cases} a \equiv b\,(mod\,n_1) \\ a \equiv b\,(mod\,n_2) \\ ------- \\ a \equiv b\,(mod\,n_k) \end{cases} \Leftrightarrow a \equiv b\,(mod\,M), \quad \text{где } M = [n_1, n_2, \ldots n_k].$$

Множество $a+n\mathbb{Z} = \{x \in \mathbb{Z} : x \equiv a\,(mod\,n)\} = \{..., a-2n, a-n, a, a+n, a+2n, \ldots\}$ всех целых чисел, сравнимых с данным числом a по модулю n, называется *классом вычетов числа* a по модулю n. При работе с конкретным модулем n вместо записи $a+nZ$ часто используют запись $\overline{a}$. Сложение и умножение на множестве $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$ всех классов вычетов определяются так: $\overline{a}+\overline{b} = \overline{a+b}$, и $\overline{a}\cdot\overline{b} = \overline{a \cdot b}$. В этом случае $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ превращается в коммутативное кольцо, содержащее n элементов. Элемент $\overline{a} \in \mathbb{Z}_n$ обратим в точности тогда, когда $(a,n)=1$. Таким образом, обратимые элементы кольца $\mathbb{Z}_n$ образуют группу порядка $\varphi(n)$. Отсюда следует

Теорема 6.1 (Теорема Эйлера)**.** *Если* $(a,n)=1$, *то* $a^{\varphi(n)} \equiv 1\,(mod\,n)$.

Для простого числа множество $\mathbb{Z}_p$ образует поле. Следовательно имеет место следующая

Теорема 6.2 (Малая теорема Ферма)**.** *Пусть* p *— простое число и* $p \nmid a$. *Тогда* $a^{p-1} \equiv 1\,(mod\,p)$.

Полной системой вычетов по модулю n называется любой набор чисел, содержащих по одному числу из каждого класса вычетов $\mathbb{Z}_n$. Набор чисел, взятых из полной системы вычетов по модулю n и взаимно простых с n, называется *приведенной системой вычетов по модулю* n.

Свойства классов вычетов:

1. $\overline{a} = \{a+nt : t \in \mathbb{Z}\}$;

2. $\overline{a} = \overline{b} \Leftrightarrow a \equiv b\,(mod\,n)$;

3. Число классов вычетов по модулю n равно n;

4. Все числа одного класса вычетов по модулю n имеют с модулем n один и тот же наибольший общий делитель: если $x \in \overline{a}$, то $(x, n) = (a, n)$;

5. Число классов вычетов по модулю n, взаимно простых с n, равно $\varphi(n)$, где φ — функция Эйлера.

6. Число классов вычетов по модулю n, являющихся делителями нуля, равно $n - \varphi(n) - 1$.

Примеры решения задач

1. Найдите остаток от деления $f(86)$ на 11, если $f(x) = 15x^3 - 33x^2 + 7$.

Решение. Для решения задачи заменим все числа остатками от деления на 11 или, что еще удобнее, наименьшими по абсолютной величине числами, сравнимыми с ними по модулю 11: $86 \equiv -2(mod\, 11)$; $15 \equiv 4\,(mod\, 11)$; $33 \equiv 0\,(mod\, 11)$, и $7 \equiv -4\,(mod\, 11)$. Тогда $f(86) \equiv -2\,(mod\, 11)$, и мы получаем цепочку сравнений $f(-2) \equiv 4(-2)^3 - 0 \cdot (-2)^2 - 4 \equiv -32 - 4 \equiv -36 \equiv -3 \equiv 8\,(mod\, 11)$. Таким образом, остаток от деления $f(86)$ на 11 равен 8.

2. Каким классам вычетов по модулю 15 принадлежат элементы класса вычетов $\overline{2}_5$?

Решение. Класс $\overline{2}_5 = \{\ldots, -3, 2, 7, \ldots\}$ разбивается на три класса по модулю 15: $\overline{2}_{15}$, $\overline{2+5}_{15} = \overline{7}_{15}$, и $\overline{2 + 2 \cdot 5}_{15} = \overline{12}_{15}$. При этом $\overline{2}_{15} = \{\ldots, -13, 2, 17, \ldots\}$, $\overline{7}_{15} = \{\ldots, -8, 7, 22, \ldots\}$ и $\overline{12}_{15} = \{\ldots, -3, 12, 27, \ldots\}$.

3. Найдите остаток от деления $2^{7^{2002}}$ на 352.

Решение. Прежде всего заметим, что остатком от деления $2^{7^{2002}}$ на 352 является такое целое число x, что $2^{7^{2002}} \equiv x\,(mod\, 352)$, $0 \le x < 352$. Поскольку $352 = 2^5 \cdot 11$, то $(2^{7^{2002}}, 352) = 2^5$. Откуда следует, что $x = 2^5 \cdot x_1$. Разделив все три части выписанного выше сравнения на 2^5 , мы получим сравнение $2^{7^{2002} - 5} \equiv x_1\,(mod\, 11)$.

Поскольку $(2, 11) = 1$, и $\varphi(11) = 10$, то $2^{10} \equiv 1\,(mod\, 11)$. Найдем остаток от деления числа $7^{2002} - 5$ на 10, то есть такое целое число y, что $7^{2002} - 5 \equiv y\,(mod\, 10)$, $0 \le y < 10$. В этом случае $2^{7^{2002}} \equiv 2^y\,(mod\, 11)$, то есть $2^y \equiv x_1\,(mod\, 11)$.

Поскольку $(7, 10) = 1$ и $\varphi(10) = 4$, то $7^4 \equiv 1\,(mod\, 10)$. Так как $2002 = 4 \cdot 500 + 2$, то $7^{2002} - 5 \equiv (7^4)^{500} \cdot 7^2 - 5 = 7^2 - 5 = 9 - 5 \equiv 4\,(mod\, 10)$. Таким образом, $y = 4$, и мы получаем сравнение $2^4 \equiv x_1\,(mod\, 11)$. Поскольку $2^4 \equiv 5\,(mod\, 11)$, то $x_1 = 5$, и $x = 2^5 \cdot x_1 = 32 \cdot 5 = 160$.

Упражнения

1. По какому модулю все целые числа сравнимы между собой? Сколько имеется классов вычетов по этому модулю? По какому модулю сравнимы числа одинаковой четности?

2. Верны ли следующие сравнения:

1) $1 \equiv -5\,(6)$; 2) $546 \equiv 0\,(13)$; 3) $8 \equiv 1\,(4)$;

4) $121 \equiv 13145\,(2)$; 5) $121347 \equiv 92817\,(10)$; 6) $31 \equiv -9\,(10)$;
7) $0 \equiv 15\,(4)$; 8) $-3 \equiv -6\,(2)$.

3. Доказать, что $a \equiv 0\,(m) \Leftrightarrow m|a$.

4. Доказать, что $a \equiv rem(a,m)\,(mod\,m)$.

5. Доказать, что следующие три условия равносильны:
1) $a \equiv b\,(m)$;
2) $m|(a-b)$;
3) существует такое $t \in \mathbb{Z}$, что $a = b + mt$.

6. Доказать, что отношение сравнения является отношением эквивалентности.

7. Верны ли сравнения:
1) $3m \equiv -1\,(m)$; 2) $(m-1)^2 \equiv 1\,(m)$; 3) $5^{1812} \equiv 1992\,(10)$;
4) $2m+1 \equiv (m+1)^2(m)$; 5) $7^{103} \equiv 3(27)$; 6) $4^{1965} \equiv 25\,(10)$;
7) $(2n+1)(2m+1) \equiv 2k\,(6)$; 8) $2+4+6+\ldots+2m \equiv 0\,(m)$.

8. Доказать, что если $ad \equiv bd(m)$ и $(d,m)=1$, то $a \equiv b\,(m)$. Будет ли верным это утверждение без условия $(d,m)=1$?

9. Доказать, что $ad \equiv bd\,(md) \Leftrightarrow a \equiv b\,(m)$.

10. Найдите остаток от деления $f(75)$ на 11, если $f(x) = x^{10} + 4x^7 - 22x^4 + 101$.

11. Найдите остаток от деления $f(55)$ на 17, если $f(x) = 35x^5 - 50x^4 + 87x + 177$.

12. Докажите, что $2^{4n+1} + 2^{4n} - 3^{n+1} \equiv 0\,(13)$ для любого натурального числа n.

13. Докажите, что $3^{3n+2} + 2^{n+4} \equiv 0\,(25)$ для любого натурального числа n.

14. Доказать, что
а) $\overline{2}_6 \cup \overline{4}_6 = \overline{2}_3$;
б) $\overline{5}_{12} \cup \overline{-1}_{12} = \overline{5}_6$.

15. Доказать, что результат операции над классами вычетов не зависит от выбора представителей в классах, учавствующих в операции.

16. Составить таблицы сложения и умножения в Z_2, Z_5, Z_6, Z_8, Z_{11}. Выписать для каждого из колец обратимые элементы и делители нуля.

17. Найти наименьший неотрицательный вычет класса $\overline{100}_4$; наименьший положительный вычет класса $\overline{100}_4$; наибольший отрицательный вычет класса $\overline{100}_4$.

18. Пусть $M = \{-5, 12, -25, 34, -46, 15\}$. Доказать, что M — полная система вычетов по модулю 6. Выделить из M приведенную систему вычетов по модулю 6.

19. Написать приведенную систему вычетов по модулю 10, по модулю 12, по модулю 14, по модулю 20.

20. По какому модулю система $\{1, 5, 7, 11\}$ является приведенной системой вычетов?

21. Доказать, что набор чисел $\{2, 4, 5, 7\}$ не является приведенной системой вычетов ни по какому модулю.

22. Выписать все обратимые элементы в кольцах $\mathbb{Z}_5$, $\mathbb{Z}_7$, $\mathbb{Z}_8$, $\mathbb{Z}_{12}$, $\mathbb{Z}_{13}$ и указать обратные к ним.

23. Выполнить вычисления в поле $\mathbb{Z}_7$:

$$1)\,\frac{\overline{1}}{\overline{3}};\qquad 2)\,\frac{\overline{2}}{\overline{5}};\qquad 3)\,1-\frac{\overline{3}}{\overline{4}};\qquad 4)\,\frac{\overline{5}^2+\overline{4}^3}{\overline{2}-\overline{6}}.$$

24. Решить уравнения в поле $\mathbb{Z}_{13}$:

$$1)\,\overline{2}x+\overline{3}=\overline{0};\quad 2)\,\overline{-11}x+\overline{12}=\overline{2}x+\overline{10};\quad 3)\,\frac{\overline{1}}{\overline{3}}x-\frac{\overline{7}}{\overline{5}}=\frac{\overline{2}}{\overline{11}}+\frac{\overline{4}}{\overline{10}}.$$

25. Решить системы уравнений в поле $\mathbb{Z}_{13}$:

1) $\begin{cases}\overline{2}x+\overline{3}y&=&\overline{5}\\ \overline{3}x+\overline{4}y&=&\overline{2}\end{cases}$ 2) $\begin{cases}\overline{2}x-\overline{3}y&=&\overline{5}\\ \overline{3}x-y&=&\overline{2}\end{cases}$ 3) $\begin{cases}\overline{2}x-\overline{3}y&=&\overline{5}\\ \overline{3}x-y&=&\overline{4}\end{cases}$

4) $\begin{cases}\overline{6}x-\overline{2}y&=&\overline{1}\\ \overline{3}x+y&=&\overline{4}\end{cases}$ 5) $\begin{cases}\overline{6}x-\overline{2}y&=&\overline{1}\\ \overline{3}x+\overline{6}y&=&\overline{3}\end{cases}$ 6) $\begin{cases}\overline{6}x-\overline{2}y&=&\overline{1}\\ \overline{3}x+\overline{6}y&=&\overline{4}\end{cases}$

26. Найдите остаток от деления:

1) 10^{10} на 13; 2) 178^{52} на 11; 3) 1967^{1968} на 11;

4) 28^{16} на 5; 5) 3^{100} на 16; 6) 31^{200} на 28.

27. Найдите две последние цифры десятичной записи числа:

1) 2^{999}; 2) 5^{2011}; 3) 123^{2010};

4) 3^{999}; 5) 7^{2011}; 6) 555^{2012}.

28. Найдите остаток от деления:

1) $5^{5^{1000}}$ на 325; 2) $4^{5^{3000}}$ на 208; 3) $5^{3^{1000}}$ на 275.

29. Пусть R — кольцо, $char R=n\neq 0$. Докажите, что R содержит подкольцо, изоморфное кольцу $\mathbb{Z}_n$.

30. Доказать, что любое поле F характеристики p содержит подполе K, изоморфное полю $\mathbb{Z}_p$ и F можно рассматривать как векторное пространство над K.

31. Найдите все идеалы в кольце $\mathbb{Z}$, $\mathbb{Z}_8$, $\mathbb{Z}_{25}$.

32. Докажите, что для любого целого числа k идеал $k\mathbb{Z}_n$ совпадает с $d\mathbb{Z}_n$, где $d=(n,k)$.

33. Опишите все идеалы кольца $\mathbb{Z}_n$.

34. Укажите все целые числа, входящие в идеалы $6\mathbb{Z}+8\mathbb{Z}$, $3\mathbb{Z}+5\mathbb{Z}$, $3\mathbb{Z}+6\mathbb{Z}$. Всегда ли выполняется равенство $J_1+J_2=J_1\cup J_2$?

35. Какие из чисел $3-5i$, $4+6i$, $-15+9i$, $5-2i$ принадлежат идеалу $(3+5i)$ кольца целых гауссовых чисел? Какие из них порождают этот идеал?

36. Укажите числа, принадлежащие одному смежному классу по идеалу (2) в кольце $\mathbb{Z}[i]$: $-3+5i$; $7-8i$; $25+3i$; $47+10i$; -2; $1+i$; $1-i$; $3i$; 1; -1; $2+i$; $-2+3i$.

37. Какие из следующих равенств имеют место в факторкольце $\mathbb{Z}[i]/(2)$:

a) $1+2i+(2)=1-2i+(2)$; *d*) $18-4i+(2)=0+(2)$;

b) $1+(2)=i+(2)$; *e*) $3-i+(2)=3+i+(2)$;

c) $3i+(2)=18-i+(2)$; *f*) $3i+(2)=2+i+(2)$?

38. Найдите все элементы факторкольца $\mathbb{Z}[i]/(2)$. Составьте таблицы сложения и умножения. Покажите, что это факторкольцо не является областью целостности.

7. Решение линейных сравнений и неопределенных уравнений

Линейное сравнение с одним неизвестным это сравнение вида

$$ax \equiv b\,(m) \tag{1}$$

Если число k удовлетворяет (1), то и любое l такое, что $l \equiv k\,(m)$, удовлетворяет (1). Поэтому решением сравнения (1) называется любой класс вычетов по модулю m, элементы которого удовлетворяют (1). Решение сравнения (1) записывается в виде $x \equiv x_0\,(m)$.

Теорема 7.1. *1) Если $(a, m) = 1$, то сравнение (1) имеет единственное решение, которое находится по формуле*

$$x \equiv a^{\varphi(m)-1} b\,(m)$$

или по формуле

$$x \equiv (-1)^{n-1} \cdot P_{n-1} \cdot b\,(m),$$

где P_{n-1} — числитель предпоследней подходящей дроби в разложении $\dfrac{m}{a}$ в цепную дробь (мы можем считать, что $a < m$, т.к. a и b можно заменить любыми числами, сравнимыми с ними по модулю m).

2) Если $(a, m) = d > 1$ и $d|b$, то сравнение (1) имеет d решений, которые находятся по формуле

$$x \equiv x_0\,(m), x \equiv x_0 + \frac{m}{d}\,(m), x \equiv x_0 + \frac{2m}{d}\,(m), \ldots, x \equiv x_0 + \frac{(d-1)m}{d}\,(m),$$

где x_0 — любое число, удовлетворяющее сравнению

$$\frac{a}{d}x \equiv \frac{b}{d}\,\left(\frac{m}{d}\right).$$

3) Если $(a, m) = d > 1$ и $d \nmid b$, то сравнение (1) не имеет решений.

Непределенным уравнением первой степени с двумя неизвестными называется уравнение вида

$$ax + by = c, \qquad \text{где} \quad a, b, c \in \mathbb{Z}. \tag{2}$$

Решением такого уравнения называется любая удовлетворяющая ему пара целых чисел (x, y). Если $(a, b) \nmid c$, то, очевидно, уравнение (2) не имеет решений. Если $(a, b) \mid c$, то сократив на (a, b), приходим к уравнению, в котором коэффициенты при x и y взаимно просты. Поэтому мы с самого начала можем отыскивать решения таких уравнений (2), у которых $(a, b) = 1$.

Теорема 7.2. *Если* $(a, b) = 1$, *то любое решение уравнения (2) находится по формулам*

$$\begin{cases} x = x_0 - bt \\ y = y_0 + at, \qquad t \in \mathbb{Z} \end{cases}$$

где x_0 *— любое число, удовлетворяющее сравнению* $ax_0 \equiv c(b)$, $y_0 = \dfrac{c - ax_0}{b}$. *Любая пара чисел* x, y, *удовлетворяющая этим условиям при некотором* $t \in \mathbb{Z}$ *есть решение уравнения (2).*

Практически для решения неопределенного уравнения (2) можно использовать метод, который мы рассмотрим в примере 2.

Теорема 7.3 (Китайская теорема об остатках)**.** *Если* $m_1, m_2, \ldots, m_k$ *— попарно взаимно простые числа, то система*

$$\begin{cases} x \equiv c_1(m_1) \\ x \equiv c_2(m_2) \\ - - - - - \\ x \equiv c_k(m_k) \end{cases} \tag{3}$$

имеет решение, причем единственное, по модулю $M = m_1 m_2 \ldots m_k$. *Для нахождения решения этой системы нужно сначала найти числа* $y_1, y_2, \ldots, y_k$, *удовлетворяющие сравнениям*

$$\frac{M}{m_1} y_1 \equiv 1(m_1), \quad \frac{M}{m_2} y_2 \equiv 1(m_2), \ldots, \quad \frac{M}{m_k} y_k \equiv 1(m_k).$$

Тогда решение системы (3) имеет вид

$$x \equiv \frac{M}{m_1} y_1 c_1 + \frac{M}{m_2} y_2 c_2 + \ldots + \frac{M}{m_k} y_k c_k (M).$$

В общем случае решением системы линейных сравнений

$$\begin{cases} x \equiv c_1(m_1) \\ - - - - - \\ x \equiv c_k(m_k) \end{cases}$$

является класс вычетов по модулю $N = [m_1, \ldots, m_k] : x \equiv \alpha(N)$.

Примеры решения задач

1. Решить сравнение $11x \equiv 5\,(7)$.

Решение. Прежде всего перепишем сравнение в виде $4x \equiv -2\,(7)$. Поскольку $(4,7) = 1$, то сравнение имеет единственное решение — класс вычетов по модулю 7. Домножая обе части сравнения $4x \equiv -2\,(7)$ на $4^{\varphi(7)-1} = 4^5$, мы получаем, что $x \equiv -2 \cdot 4^5\,(7)$. Поскольку $4^5 = (-3)^5 \equiv 9 \cdot (-27) \equiv 2 \cdot 1 \equiv 2\,(7)$, то $x \equiv -2 \cdot 2 \equiv -4 \equiv 3\,(7)$.

Решим сравнение с помощью цепных дробей. Для этого разложим число $\dfrac{7}{4}$ в цепную дробь. Имеем: $\dfrac{7}{4} =< 1, 1, 3 >$, $n = 3$. Откуда находим $P_2 = 2$. Следовательно, $x \equiv (-1)^{3-1} \cdot 2 \cdot (-2) \equiv 3\,(7)$.

2. Решить неопределенное уравнение

$$12x + 7y = 1. \qquad (i)$$

Решение. Левую часть разделим на наименьший коэффициент и возьмем неполные частные. Полученное выражение обозначим новой переменной z:

$$x + y = z$$

Это выражение умножим на 7 и вычтем из уравнения (i):

$$5x = 1 - 7z$$

$$5x + 7z = 1 \qquad (ii)$$

Получили новое неопределенное уравнение, в котором минимальный элемент меньше, чем в (i). Теперь левую часть (ii) делим на наименьший коэффициент и обозначаем буквой t:

$$x + z = t$$

Умножим на 5 и вычтем из (ii):

$$2z = 1 - 5t \quad \Rightarrow \quad 2z + 5t = 1 \quad (iii)$$

Аналогично поступаем с уравнением (iii):

$$z + 2t = u$$

$$t = 1 - 2u$$

Далее,

$$z = u - 2t = 5u - 2$$

$$\begin{cases} x = t - z = 3 - 7u \\ y = z - x = 12u - 5, \; u \in \mathbb{Z} \end{cases}$$

Полученные формулы дают решение уравнения (i).

3. Решите систему сравнений первой степени

$$\begin{cases} 2x \equiv 14\,(10) \\ 15x \equiv 6\,(12) \end{cases}$$

Решение. Легко видеть, что $[10,12] = 60$. Поскольку $15x \equiv 6\,(12)$, то $3x \equiv 6\,(12)$ и $x \equiv 2\,(4)$. Далее, если $2x \equiv 14\,(10)$, то $2x \equiv 4\,(10)$, и $x \equiv 2\,(5)$. Таким образом, получим систему

$$\begin{cases} x \equiv 2\,(5) \\ x \equiv 2\,(4). \end{cases}$$

Решим ее. Имеем: $M = 4 \cdot 5 = 20$. Далее, $\dfrac{M}{m_1} = \dfrac{20}{5} = 4$; $\dfrac{M}{m_2} = \dfrac{20}{4} = 5$. Откуда

$$4y_1 \equiv 1(5) \quad \Rightarrow \quad y_1 \equiv -1\,(5);$$

$$5y_2 \equiv 1(4) \quad \Rightarrow \quad y_2 \equiv 1\,(4).$$

Тогда

$$x \equiv 4 \cdot (-1) \cdot 2 + 5 \cdot 1 \cdot 2 = 2\,(20).$$

Поскольку один класс $x \equiv 2\,(20)$ по модулю 60 разбивается на три класса $x \equiv 2\,(60)$, $x \equiv 2{+}20\,(60)$, $x \equiv 2{+}2{\cdot}20\,(60)$, то мы получаем три решения $x \equiv 2\,(60)$, $x \equiv 22\,(60)$, $x \equiv 42\,(60)$ первоначальной системы сравнений.

Упражнения

1. Решить сравнения первой степени с одним неизвестным:

$$1)\, 29x \equiv 1\,(17); \quad 2)\, 21x + 5 \equiv 0\,(29); \quad 3)\, 7x \equiv 15\,(9); \quad 4)\, 7x \equiv 9\,(10);$$

$$5)\, (a+b)x \equiv a^2 + b^2\,(ab),\; (a,b) = 1; \quad 6)\, (a^2+b^2)x \equiv a - b\,(ab),\; (a,b) = 1;$$

$$7)\, (a+b)^2 x \equiv a^2 - b^2\,(ab),\; (a,b) = 1; \quad 8)\, 2x \equiv 1\,(p), \text{ где } p - \text{простое};$$

$$9)\, 72x \equiv 2\,(10); \qquad 10)\, 8x \equiv 20\,(12); \quad 11)\, 6x \equiv 27\,(12);$$

$$12)\, 10x \equiv 15\,(35); \quad 13)\, (m-1)x \equiv 1\,(m); \quad 14)\, (m+1)^2 x \equiv a\,(m);$$

$$15)\, ax \equiv 1\,(p), \text{ где } p \nmid a,\; p - \text{простое}; \quad 16) (a+1) \equiv a^2 - 1\,(m).$$

2. Исследовать систему сравнений

$$\begin{cases} a_1x + b_1y \equiv c_1\,(m) \\ a_2x + b_2y \equiv c_2\,(m) \end{cases}$$

3. Решить в целых числах неопределенные уравнения:

$$1)\, 5x + 4y = 3; \quad 2)\, 17x + 13y = 1; \quad 3)\, 91x - 28y = 35;$$

$$4)\, 2x + 3y = 4; \quad 5)\, 4x - 3y = 2.$$

4. На прямой $8x - 13y + 6 = 0$ найти число целых точек, лежащих между прямыми $x = -100$ и $x = 150$.

5. Доказать, что внутри прямоугольника, ограниченного прямыми $x = -2$, $x = 5$, $y = -1$, $y = 2$ на прямой $3x - 7y - 1 = 0$ не лежит ни одной целой точки.

6. Какие две цифры следует приписать к числу 32, чтобы полученное число делилось на 3 и на 7?

7. Для перевозки зерна имеются мешки по 60 кг и по 80 кг. Сколько нужно тех и других мешков для перевозки 440 кг зерна?

8. Сколько билетов по 30 руб. и по 50 руб. можно купить на 1490 руб.?

9. Сколько почтовых марок по 3$ и по 4$ можно купить на 50$?

10. На станцию прибыло 500 т угля в 18 вагонах. В вагонах было по 15, 20 и 30 т угля. Сколько вагонов было по 15 т, сколько по 20 т и сколько по 30 т?

11. Ученику прислали задание, состоящее из 20 задач. За каждую верно решенную задачу ему ставят 8 баллов, за каждую неверно решенную — минус 5 баллов, за задачу, которую он не брался решать — 0 баллов. Ученик получил в сумме 13 баллов. Сколько задач он брался решать?

12. Можно ли разменять 25 руб. на рублевые, трехрублевые и пятирублевые монеты так, чтобы получить всего 10 монет?

13. Один мастер делает на длинной ленте пометки синим карандашом от ее начала через каждые 36 см, другой — красным карандашом через каждые 25 см. Может ли синяя пометка оказаться на расстоянии 1 см от какой-нибудь красной?

14. Про некоторою фигуру на плоскости известно, что при повороте вокруг точки 0 на угол 48^o она переходит в себя. Можно ли утверждать, что она переходит в себя при повороте вокруг точки 0 на угол a) 90^o; b) 72^o?

15. Ста абитуриентам роздали 480 листов бумаги, причем каждому юноше дали на 2 листа меньше, чем девушке. Сколько было девушек и юношей?

16. Найти все числа, на которые может быть сократима дробь

$$\frac{5l + 6}{8l + 7}, \quad l \in \mathbb{Z}$$

При каких значениях l дробь может быть сократима?

17. Задача Леонардо Фибоначчи (XII в.).

Некто купил 30 птиц за 30 монет. За каждые 3 воробья платил 1 монету, за каждые 2 снегиря — 1 монету, за каждого голубя — 2 монеты. Сколько было птиц каждого вида?

18. Решить следующие системы сравнений:

$$1) \begin{cases} x \equiv 2\,(5) \\ x \equiv 8\,(11) \end{cases} \qquad 2) \begin{cases} 4x \equiv 3\,(7) \\ 5x \equiv 4\,(6) \end{cases} \qquad 3) \begin{cases} 17x \equiv 7\,(2) \\ 2x \equiv 1\,(3) \\ 2x \equiv 2\,(5) \end{cases}$$

4) $\begin{cases} 3x \equiv 5\,(7) \\ 2x \equiv 3\,(5) \\ 3x \equiv 3\,(9) \end{cases}$ 5) $\begin{cases} 5x \equiv 2\,(3) \\ x \equiv 3\,(2) \\ x \equiv -1\,(6) \end{cases}$ 6) $\begin{cases} x \equiv a\,(7) \\ x \equiv b\,(5) \\ x \equiv c\,(3) \end{cases}$

19. Найти все натуральные числа, дающие при делении на 2, на 3 и на 4 в остатке 1 и делящиеся на 5 без остатка.

20. Найти все целые числа, которые при делении на 2, на 3, на 4, на 5, на 6 и на 7 дают соответственно остатки 1, 2, 3, 4, 5 и 0.

21. Между 200 и 500 найти все целые числа, которые при делении на 4, 5 и 7 дают соответственно остатки 3, 4 и 5.

22. (Старинная французская задача)

Женщина несла на рынок корзину яиц. Прохожий нечаянно толкнул и разбил яйца. Желая возместить ущерб, он спросил, сколько было яиц. — Точно не помню. Когда я вынимала из корзины по 2, 3, 4, 5, 6 яиц, в корзине оставалось одно яйцо, а когда вынимала по 7 — ничего не оставалось. Сколько было яиц?

23. Перед новым годом профком готовил подарки для детей. Когда стали раскладывать мандарины в пакеты по 10 штук — осталось 9, стали раскладывать по 9 — осталось 8, по 8 — осталось 7, по 7 — осталось 6, по 6 — осталось 5, по 5 — осталось 4, по 4 — осталось 3, по 3 — осталось 2, по 2 — осталось 1. Сколько было мандаринов?

8. Квадратичные вычеты

Число a, взаимно простое с p, где p — простое нечетное число, называется *квадратичным вычетом по модулю* p, если сравнение $x^2 \equiv a(p)$ имеет решение. В противном случае a называется *квадратичным невычетом по модулю* p. Для определения, является ли a квадратичным вычетом по модулю p, служит *символ Лежандра*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{если } a \text{ квадратичный вычет по модулю } p; \\ -1, & \text{если } a \text{ квадратичный невычет по модулю } p; \\ 0, & \text{если } p \text{ делит } a. \end{cases}$$

Таким образом, с помощью символа Лежандра легко выяснить, сколько решений имеет сравнение $x^2 \equiv a(p)$, где $p \neq 2$: если $\left(\frac{a}{p}\right) = 1$, то сравнение $x^2 \equiv a(p)$ имеет два решения: $x \equiv \pm x_0\,(p)$; если $\left(\frac{a}{p}\right) = -1$, то сравнение $x^2 \equiv a(p)$ не имеет решений; если $\left(\frac{a}{p}\right) = 0$, то сравнение $x^2 \equiv a(p)$ имеет одно решение: $x \equiv 0\,(p)$.

Симмвол Лежандра обладает следующими свойствами:

1) $a \equiv a_1(p) \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right)$;

2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

3) $\left(\frac{b^2}{p}\right) = 1$;

4) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{1}{p}\right) = 1$;

5) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$;

6) $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)$,

7) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}\,(p) \qquad$ (Критерий Эйлера),

где p — простое нечетное число. Свойство (6) называется квадратичным законом взаимности. Перечисленные свойства позволяют легко вычислить символ Лежандра (см. пример 1).

Пусть b — нечетное положительное целое число и a — произвольное целое число. Пусть $b = p_1 p_2 \dots p_m$, где p_i — (не обязательно различные) простые числа. Символ $\left(\dfrac{a}{b}\right)$, определённый формулой

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_m}\right),$$

называется *символом Якоби.*

Свойства символа Якоби очень близки к свойствам символа Лежандра, который он обобщает. Будет полезно, однако, сделать одно предупреждение. Символ $\left(\dfrac{a}{b}\right)$ может быть равным 1 и тогда, когда a не является квадратичным вычетом по модулю b. Например, $\left(\dfrac{2}{15}\right) = \left(\dfrac{2}{3}\right)\left(\dfrac{2}{5}\right) = (-1)\cdot(-1) = 1$, но 2 не является квадратичным вычетом по модулю 15. Верно, однако, что если $\left(\dfrac{a}{b}\right) = -1$, то a не будет квадратичным вычетом по модулю b. Таким образом, с помощью символа Якоби можно получить подтверждение неразрешимости сравнения $x^2 \equiv a(n)$: если $\left(\dfrac{a}{n}\right) = -1$, то сравнение $x^2 \equiv a(n)$ не имеет решений.

Свойства символа Якоби:

1) $\left(\dfrac{a_1}{b}\right) = \left(\dfrac{a_2}{b}\right)$, если $a_1 \equiv a_2(b)$;

2) $\left(\dfrac{a_1 a_2}{b}\right) = \left(\dfrac{a_1}{b}\right)\left(\dfrac{a_2}{b}\right)$;

3) $\left(\dfrac{a}{b_1 b_2}\right) = \left(\dfrac{a}{b_1}\right)\left(\dfrac{a}{b_2}\right)$.

Примеры решения задач

1. Вычислить $\left(\dfrac{37}{67}\right)$.

Решение. По свойству 6)

$$\left(\frac{37}{67}\right) = (-1)^{\frac{37-1}{2}\cdot\frac{67-1}{2}}\left(\frac{67}{37}\right) = \left(\frac{67}{37}\right).$$

Поскольку $67 \equiv 30 (37)$, то по свойству 1) имеем $\left(\dfrac{67}{37}\right) = \left(\dfrac{30}{37}\right)$. Далее, применив свойство 2), получим

$$\left(\frac{30}{37}\right) \equiv \left(\frac{2}{37}\right) \cdot \left(\frac{3}{37}\right) \cdot \left(\frac{5}{37}\right).$$

Откуда по свойству 5): $\left(\dfrac{2}{37}\right) = (-1)^{\frac{37^2-1}{8}} = -1$. Теперь по свойству 6):

$$\left(\frac{3}{37}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{37-1}{2}} \left(\frac{37}{3}\right) = \left(\frac{37}{3}\right) = \left(\frac{1}{3}\right) = 1;$$

$$\left(\frac{5}{37}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{37-1}{2}} \left(\frac{37}{5}\right) = \left(\frac{37}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1.$$

Итак, $\left(\dfrac{37}{67}\right) = (-1)\cdot 1 \cdot (-1) = 1$.

2. Вычислить $\left(\dfrac{37}{67}\right)$ при помощи символа Якоби.

Решение. Имеем

$$\left(\frac{37}{67}\right) = \left(\frac{67}{37}\right) = \left(\frac{30}{37}\right) = \left(\frac{2}{37}\right) \cdot \left(\frac{15}{37}\right) = -\left(\frac{15}{37}\right) = -(-1)^{\frac{37-1}{2}\cdot\frac{15-1}{2}} \left(\frac{37}{15}\right) =$$

$$= -\left(\frac{37}{15}\right) = -\left(\frac{7}{15}\right) = -(-1)^{\frac{15-1}{2}\cdot\frac{7-1}{2}} \left(\frac{15}{7}\right) = \left(\frac{15}{7}\right) = \left(\frac{1}{7}\right) = 1.$$

3. Докажите, что сравнение $ax^2 + bx + c \equiv 0\,(p)$, $p \neq 2$, $(a, p) = 1$, имеет два решения, если $\left(\dfrac{D}{p}\right) = 1$; одно решение, если $\left(\dfrac{D}{p}\right) = 0$; не имеет решений, если $\left(\dfrac{D}{p}\right) = -1$, где $D = b^2 - 4ac$.

Решение. Так как p — нечетно, то можно провести ряд равносильных преобразований: $ax^2 + bx + c \equiv 0\,(p) \Leftrightarrow 4a^2x^2 + 4abx + 4ac \equiv 0\,(p) \Leftrightarrow (2ax+b)^2 - b^2 + 4ac \equiv 0\,(p) \Leftrightarrow (2ax+b)^2 \equiv b^2 - 4ac\,(p)$. В итоге сравнение $ax^2 + bx + c \equiv 0\,(p)$ равносильно сравнению $y^2 \equiv b^2 - 4ac\,(p)$, или, что то же, сравнению $y^2 \equiv D\,(p)$. Таким образом, если $\left(\dfrac{D}{p}\right) = 1$, то сравнение $y^2 \equiv D\,(p)$ имеет два решения, и им соответствуют два решения сравнения $ax^2 + bx + c \equiv 0\,(p)$; если $\left(\dfrac{D}{p}\right) = -1$, то сравнение

$y^2 \equiv D\,(p)$ не имеет решений, и равносильное ему сравнение $ax^2+bx+c \equiv 0\,(p)$ также неразрешимо; наконец, если $\left(\dfrac{D}{p}\right) = 0$, то сравнение $y^2 \equiv D\,(p)$ имеет единственное нулевое решение и ему соответствует единственное решение сравнения $ax^2+bx+c \equiv 0\,(p)$.

4. Для каких простых р число 5 является квадратичным невычетом?

Решение. Очевидно, что $p \neq 2$ и $p \neq 5$. Далее, для $p \neq 2, 5$ имеет место соотношение $\left(\dfrac{5}{p}\right) = \left(\dfrac{p}{5}\right)$. Если $p \equiv 1\,(5)$, то $\left(\dfrac{p}{5}\right) = \left(\dfrac{1}{5}\right) = 1$. Если $p \equiv -1\,(5)$, то $\left(\dfrac{p}{5}\right) = \left(\dfrac{-1}{5}\right) = 1$. Если $p \equiv 2\,(5)$, то $\left(\dfrac{p}{5}\right) = \left(\dfrac{2}{5}\right) = -1$. Если $p \equiv -2\,(5)$, то $\left(\dfrac{p}{5}\right) = \left(\dfrac{-2}{5}\right) = \left(\dfrac{-1}{5}\right)\left(\dfrac{2}{5}\right) = 1\cdot(-1) = -1$. Таким образом, $\left(\dfrac{p}{5}\right) = -1$ и, следовательно, 5 является квадратичным невычетом по модулю р, для нечетных простых $p \equiv \pm 2\,(5)$, то есть для $p = \{3, 7, 13, 17, 23, 37, 43, 47, \ldots\}$.

Упражнения

1. Привести примеры, когда символ Якоби $\left(\dfrac{a}{m}\right) = 1$, но сравнение $x^2 \equiv a(m)$ не имеет решений.

2. Вычислить символ Лежандра

$$1)\ \left(\frac{13}{7}\right),\quad 2)\ \left(\frac{22}{13}\right),\quad 3)\ \left(\frac{426}{491}\right)\quad 4)\ \left(\frac{-125}{47}\right).$$

3. При помощи символа Лежандра выяснить, какие из следующих сравнений разрешимы:

$$1)\, x^2 \equiv 5\,(19);\quad 2)\, x^2 \equiv 5\,(29);\quad 3)\, x^2 \equiv 2\,(97);\quad 4)\, x^2 \equiv 241\,(587);$$

$$5)\, x^2 \equiv 151\,(587);\quad 6)\, x^2 \equiv 903\,(2111);\quad 7)\, x^2 \equiv 219\,(383);\quad 8)\, x^2 \equiv 7\,(1964).$$

4. Доказать, что произведение двух последовательных натуральных чисел при делении на 13 не может давать в остатке 1.

5. Доказать, что следующие сравнения разрешимы при любом простом $p > 2$:
1) $(x^2-13)(x^2-17)(x^2-221) \equiv 0\,(p)$;
2) $(x^2-3)(x^2-5)(x^2-7)(x^2-11)(x^2-1155) \equiv 0\,(p)$.

6. Решите сравнение $x^2-6x+7 \equiv 0\,(31)$.

7. Укажите число решений сравнений:
1) $2x^2+7x+5 \equiv 0\,(37)$; 2) $3x^2+5x+7 \equiv 0\,(87)$;

3) $2x^2 - 3x + 4 \equiv 0\,(151)$;   4)$168x^2 + 169x + 84 \equiv 0\,(503)$.

8. Для каких простых p число 3 является квадратичным невычетом?

9. Для каких простых p число 7 является квадратичным невычетом?

10. Если простое число $p = 4k + 3$, то из чисел a и $-a$ одно является квадратичным вычетом, а другое — невычетом по модулю p; если же $p = 4k + 1$, то либо a и $-a$ — оба квадратичные вычеты, либо оба невычеты.

9. Первообразные корни и индексы. Решение степенных сравнений

Пусть $\mathbb{Z}_n$ — кольцо вычетов по модулю n, $U(\mathbb{Z}_n)$ — группа обратимых элементов кольца $\mathbb{Z}_n$.

Теорема 9.1. *Элемент $\overline{a} \in \mathbb{Z}_n$ обратим тогда и только тогда, когда $(a, n) = 1$. В $\mathbb{Z}_n$ имеется в точности $\varphi(n)$ обратимых элементов. Кольцо $\mathbb{Z}_n$ является полем в том и только том случае, когда n — простое число.*

Следствие 9.1 (Теорема Эйлера)**.** *Если $(a, n) = 1$, то $a^{\varphi(n)} \equiv 1\,(n)$.*

Из китайской теоремы об остатках, применительно к теории колец следует

Теорема 9.2.
$$U(\mathbb{Z}_n) \cong U(\mathbb{Z}_{p_1^{\alpha_1}}) \times \ldots \times U(\mathbb{Z}_{p_m^{\alpha_m}}),$$
где $n = p_1^{\alpha_1} \ldots p_m^{\alpha_m}$.

Следовательно, для определения структуры группы $U(\mathbb{Z}_n)$ достаточно рассмотреть случай $U(\mathbb{Z}_{p^\alpha})$, где p — простое число.

Теорема 9.3. *Если p — нечетное простое число и $n \in \mathbb{Z}^+$, то $U(\mathbb{Z}_{p^n})$ — циклическая группа. Группа $U(\mathbb{Z}_{2^n})$ для $n > 2$ является прямым произведением двух циклических групп, одной порядка 2, другой порядка 2^{m-2}.*

Пусть $a, n \in \mathbb{Z}$. Число a называется *первообразным корнем по модулю n*, если класс вычетов a по модулю n порождает группу $U(\mathbb{Z}_n)$. Это эквивалентно требованию, чтобы a и n были взаимно просты и чтобы $\varphi(n)$ было наименьшим положительным целым числом, для которого $a^{\varphi(n)} \equiv 1\,(n)$.

Из теорем 9.2 и 9.3 получается ряд следствий.

Следствие 9.2. *Число n обладает первообразными корнями в точности тогда, когда оно имеет вид 2, 4, p^α или $2p^\alpha$, где p — нечетное простое число.*

Следствие 9.3. *Пусть a является первообразным корнем по модулю n. Тогда $\{1, a, a^2, \ldots, a^{\varphi(n)-1}\}$ — приведенная система вычетов по модулю n.*

Следствие 9.4. *Если a — первообразный корень по модулю n, то*
$$a^{m_1} \equiv a^{m_2} \quad \Leftrightarrow \quad m_1 \equiv m_2\,(\varphi(n)).$$

Пусть a — первообразный корень по модулю n и $(b, n) = 1$. По следствию 9.3 существует такое $s \in \{0, 1, 2, \ldots, \varphi(n) - 1\}$, что $a^s \equiv b\,(n)$. По следствию 9.4 это число s единственно. Оно называется *индексом b по основанию a* и обозначается $ind_a^n b$. Там где это не ведет к недоразумениям, символы a и n в этом обозначении опускаются. Для сравнительно небольших n вида p^α составлены таблицы индексов, которые можно найти в учебниках.

Как видно из определения, индексы являются аналогами логарифмов. Их свойства также аналогичны свойствам логарифмов:

1) Если $a \equiv b\,(n)$, то $ind\,a \equiv ind\,b\,(\varphi(n))$;
2) $ind\,(bc) \equiv ind\,b + ind\,c\,(\varphi(n))$;
3) $ind\,b^m \equiv m \cdot ind\,b\,(\varphi(n))$.

Эта теорема широко используется при решении степенных и показательных сравнений, в том числе сравнения вида $x^n \equiv b\,(m)$, где m — произвольное нечетное число (не обязательно имеющее вид p^α). Решение таких сравнений основано на следующей теореме.

Теорема 9.4. *Пусть $m_1, m_2, \ldots, m_k$ — попарно взаимно простые числа, $m = m_1 \cdot m_2 \cdot \ldots \cdot m_k$, $F(x)$ — многочлен с целыми коэффициентами. Пусть $x_1, x_2, \ldots, x_k$ — решения сравнений*

$$F(x) \equiv 0\,(m_1),\; F(x) \equiv 0\,(m_2), \ldots,\; F(x) \equiv 0\,(m_k)$$

соответственно, y — решение системы сравнений

$$\begin{cases} y \equiv x_1(m_1) \\ y \equiv x_2(m_2) \\ -\,-\,-\,-\,- \\ y \equiv x_k(m_k) \end{cases}$$

(такое решение существует в силу китайской теоремы об остатках). Тогда y — решение сравнения

$$F(x) \equiv 0\,(m) \tag{1}$$

и всякое решение сравнения (1) получается таким образом.

Примеры решения задач

1. Составить таблицы индексов по модулю 3, по модулю 9, по модулю 5, по модулю 25.

Решение.

1) Пусть $n = 3$, тогда $\varphi(3) = 2$. Очевидно, что 2 — первообразный корень по модулю 3:

$$2^0 \equiv 1\,(3), \quad 2^1 \equiv 2(3), \text{ т.е. } \quad ind_2^3 1 = 0, \quad ind_2^3 2 = 1.$$

В верхней строке таблицы выписываются все числа взаимно простые с модулем, в нижней — их индексы

$$(n = 3, a = 2)$$

b	1	2
$ind\, b$	0	1

2) Пусть $n = 9$, тогда $\varphi(9) = 6$. Имеем

$$2^0 \equiv 1\,(9),\ 2^1 \equiv 2\,(9),\ 2^2 \equiv 4\,(9),\ 2^3 \equiv 8\,(9),\ 2^4 \equiv 7\,(9),\ 2^5 \equiv 5\,(9),$$

т.е. при $1 \le k < \varphi(9)\quad 2^k \not\equiv 1\,(9)$ Таким образом, 2 — первообразный корень по модулю 9.

$$(n = 9, a = 2)$$

b	1	2	4	5	7	8
$ind\, b$	0	1	2	5	4	3

3) Пусть $n = 5$, тогда $\varphi(5) = 4$.

$$2^0 \equiv 1\,(5),\ 2^1 \equiv 2\,(5),\ 2^2 \equiv 4\,(5),\ 2^3 \equiv 3\,(5).$$

Следовательно, 2 — первообразный корень по модулю 5.

$$(n = 5, a = 2)$$

b	1	2	3	4
$ind\, b$	0	1	3	2

4) Пусть $n = 25$, тогда $\varphi(25) = 20$. Имеем $2^0 \equiv 1\,(25)$, $2^1 \equiv 2\,(25)$, $2^2 \equiv 4\,(25)$, $2^3 \equiv 8\,(25)$, $2^4 \equiv 16\,(25)$, $2^5 \equiv 7\,(25)$, $2^6 \equiv 14\,(25)$, $2^7 \equiv 3\,(25)$, $2^8 \equiv 6\,(25)$, $2^9 \equiv 12\,(25)$, $2^{10} \equiv -1\,(25)$, $2^{11} \equiv -2\,(25)$, $2^{12} \equiv -4\,(25)$, $2^{13} \equiv -8\,(25)$, $2^{14} \equiv 9\,(25)$, $2^{15} \equiv 18\,(25)$, $2^{16} \equiv 11\,(25)$, $2^{17} \equiv 22\,(25)$, $2^{18} \equiv 19\,(25)$, $2^{19} \equiv 13\,(25)$.

Следовательно, 2 — первообразный корень по модулю 25.

Таблица индексов имеет вид

$$(n = 25, a = 2)$$

b	1	2	3	4	6	7	8	9	11	12	13	14	16
$ind\, b$	0	1	7	2	8	5	3	14	16	9	19	6	4

17	18	19	21	22	23	24
13	15	18	12	17	11	10

2. Решить сравнение $\quad 3x^5 \equiv 4\,(25)$.

Решение. Переходим к индексам: $ind\,(3x^5) = ind\, 4$. По свойствам индексов

$$ind\, 3 + 5 \cdot ind\, x \equiv ind\, 4\,(20).$$

Обозначим $ind\,x = y$, $ind\,3$ и $ind\,4$ найдем по таблице из предыдущего примера: $ind\,3 = 7$, $ind\,4 = 2$. Получаем сравнение $7 + 5y \equiv 2\,(20)$ или $5y \equiv 15\,(20)$. Отсюда $y \equiv 3\,(4)$, т.е.

$$y \equiv 3\,(20),\;\; y \equiv 7\,(20),\;\; y \equiv 11\,(20),\;\; y \equiv 15\,(20),\;\; y \equiv 19\,(20).$$

Тогда

$$ind\,x = 3,\;\; ind\,x = 7,\;\; ind\,x = 11,\;\; ind\,x = 15,\;\; ind\,x = 19.$$

Из таблицы индексов находим

$$x \equiv 8\,(25),\;\; x \equiv 3\,(25),\;\; x \equiv 23\,(25),\;\; x \equiv 18\,(25),\;\; x \equiv 13\,(25).$$

3. Решить сравнение $3^x \equiv 12\,(25)$.

Решение. Переходя к индексам, получаем

$$x \cdot ind\,3 \equiv ind\,12\,(20) \quad \Rightarrow \quad 7x \equiv 9\,(20) \quad \Rightarrow \quad x \equiv 7\,(20).$$

Отметим, что если полученное для индексов сравнение не имеет решения, то не имеет решения и исходное сравнение.

4. Решить сравнение $x^3 \equiv 8\,(225)$.

Решение. Имеем $225 = 3^2 \cdot 5^2$. Поэтому рассмотрим сначала следующие сравнения:

$$x^3 \equiv 8\,(9), \quad x^3 \equiv 8\,(25)$$

a)

$$x^3 \equiv 8\,(9) \;\Rightarrow\; 3 \cdot ind\,x \equiv ind\,8\,(6),\, ind\,x = z, \Rightarrow\; 3z \equiv 3\,(6), \;\Rightarrow\; z \equiv 1\,(2),$$

т.е. $z = 1,\; z = 3,\; z = 5$ и $x \equiv 2\,(9),\; x \equiv 8\,(9),\; x \equiv 5\,(9)$.

b)

$$x^3 \equiv 8\,(25) \;\Rightarrow\; 3 \cdot ind\,x \equiv ind\,8\,(20),\, ind\,x = 1, \Rightarrow\; x \equiv 2\,(25).$$

Теперь, ввиду теоремы 9.4, нужно рассмотреть три следующие системы сравнений:

1) $\begin{cases} x \equiv 2(9) \\ x \equiv 2(25) \end{cases}$ 2) $\begin{cases} x \equiv 8(9) \\ x \equiv 2(25) \end{cases}$ 3) $\begin{cases} x \equiv 5(9) \\ x \equiv 2(25) \end{cases}$

Решая эти системы при помощи китайской теоремы об остатках, получаем следующие решения исходного сравнения:

$$x \equiv 2(225), \quad x \equiv 152(225), \quad x \equiv 77(225).$$

5. Найти остаток от деления 1985^{1985} на 9.

Решение. Пусть $x \equiv 1985^{1985}\,(9)$, тогда

$$x \equiv 5^{1985}\,(9) \;\Rightarrow\; ind\,x \equiv 1985 \cdot ind\,5\,(6) \;\Rightarrow$$

$$\Rightarrow\; ind\,x \equiv -ind\,5\,(6) \;\Rightarrow\; ind\,x \equiv -5\,(6),$$

т.е. $ind\,x \equiv 1\,(6)$, $x \equiv 2\,(9)$. Таким образом, остаток от деления 1985^{1985} на 9 равен 2.

Упражнения

1. Найти первообразные корни и составить таблицы индексов по модулям 7, 11, 13, 49.

2. Докажите, что первообразных корней по модулю 12 не существует.

3. Пусть G — мультипликативная группа классов вычетов, взаимно простых с простым числом p, и C — аддитивная группа классов вычетов по модулю $p-1$. Покажите, что отображение $a\,mod\,p \to ind\,a\,mod\,(p-1)$ является изоморфизмом группы G на группу C.

4. Пользуясь таблицами индексов, найдите

а) порядок 7 по модулю 29;

б) порядок 13 по модулю 47;

в) порядок 18 по модулю 41.

(Указание. Вспомните формулу $ord\,g^k = \frac{ord\,g}{(k, ord\,g)}$ для вычисления порядка элемента в группе).

5. Доказать, что произведение двух первообразных корней модуля $p > 2$ не может быть первообразным корнем этого модуля.

6. Можно ли написать 12 чисел 1, 2, 3, ... , 12 по окружности так, чтобы для любых трех чисел a, b, c, стоящих подряд, число $b^2 - ac$ делилось на 13?

7. Решить следующие сравнения:

$$1)\,3x^{12} \equiv 4\,(5); \quad 2)\,x^2 \equiv 3\,(11); \quad 3)\,13x^{21} \equiv 5\,(9);$$

$$4)\,3x^5 \equiv 7\,(25); \quad 5)\,x^5 \equiv 25\,(13); \quad 6)\,3x^{15} \equiv 4\,(25);$$

$$7)\,x^5 \equiv 20\,(7); \quad 8)\,x^6 \equiv 9\,(11); \quad 9)\,3x^8 \equiv 5\,(13);$$

8. Решить следующие сравнения:

$$1)\,4^x \equiv 1\,(3); \quad 2)\,5^x \equiv 1\,(9); \quad 3)\,3^x \equiv 1\,(25);$$

$$4)\,6^x \equiv 1\,(49); \quad 5)\,21^{3x} \equiv 21^5\,(29); \quad 6)\,13^x \equiv 5\,(11).$$

9. Решить сравнения:

$$1)\,x^{13} \equiv 47\,(105); \quad 2)\,x^4 \equiv 7\,(225); \quad 3)\,2x^6 \equiv 5\,(13).$$

10. Найти остаток от деления:

$$10^{10}\text{ на }13; \quad 178^{52}\text{ на }11; \quad 1967^{1968}\text{ на }11; \quad 28^{16}\text{ на }5.$$

10. Литература

1. Задачи и упражнения по теории чисел. Часть 1. – Н.Новгород.: ННГУ, 1995. – 29 с.
2. Задачи и упражнения по теории чисел. Часть 2. – Н.Новгород.: ННГУ, 1995. – 32 с.
3. Виноградов И.М. Основы теории чисел. – Учебное пособие. – СПб.: Лань, 2006. – 176 с.
4. Бухштаб, А.А. Теория чисел. – М.: Просвещение, 1966. – 385 с.
5. Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел/ Пер. с англ. С.П. Демушкина. Под ред. А.Н. Паршина. – М.: Мир, 1987. – 415 с.
6. Деза Е.И., Котова Л.Е. Сборник задач по теории чисел (112 задач с подробными решениями): Учебное пособие. – М.: Либроком, 2012. – 224 с.
7. Кудреватов Г.А. Сборник задач по теории чисел. – М.: Просвещение, 1970. – 128 с.
8. Куликов Л.Я., Москаленко А.И., Фомин А.А. Сборник задач по алгебре и теории чисел. – М.: Просвещение, 1993. – 288 с.
9. Кузьмичёв А.И., Тропин М.П. Теория чисел. Задачник-практикум. – Новосибирск: НГПУ (Новосибирский Государственный Педагогический Университет), 2009. – 119 с.
10. Эвнин А.Ю. Мультипликативные функции в теории чисел// Математика в высшем образовании. – 2008. – № 6. – С. 89–98.

Михаил Иванович **Кузнецов**
Олег Владимирович**Любимцев**

Задачи по теории чисел

Учебно-методическое пособие

Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский Нижегородский государственный
университет им. Н.И. Лобачевского».
603950, Нижний Новгород, пр. Гагарина, 23