Уральский федеральный университет
имени первого Президента России Б.Н.Ельцина
Институт радиоэлектроники и информационных технологий

Б. М. ВЕРЕТЕННИКОВ
М. М. МИХАЛЕВА

АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ

Часть I

Учебное пособие

Министерство образования и науки Российской Федерации
Уральский федеральный университет
имени первого Президента России Б. Н. Ельцина

Б. М. Веретенников, М. М. Михалева

АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ

Часть I

Рекомендовано методическим советом УрФУ
*в качестве **учебного пособия** для студентов,*
обучающихся по направлению подготовки
010500.68 – Теоретические основы информатики

Екатеринбург
Издательство Уральского университета
2014

УДК 511+512(075.8)
ББК 22.13я73+22.14я73
В31

Рецензенты:
кафедра Прикладной математики Уральского государственного экономического университета; протокол №1 от 29.08.2013 г. (завкафедрой, канд. физ.-мат. наук, доц. Ю. Б. Мельников);
И. Н. Белоусов, канд. физ.-мат. наук (Институт математики и механики УрО РАН)

Научный редактор – канд. физ.-мат. наук, доц. Н. В. Чуксина

Веретенников, Б. М.
В31 Алгебра и теория чисел : учебное пособие / Б. М. Веретенников, М. М. Михалева. – Екатеринбург : Изд-во Урал. ун-та, 2014. – Ч. 1. – 52 с.
ISBN 978-5-7996-1193-4 (ч. 1)
ISBN 978-5-7996-1166-8

Учебное пособие включает в себя такие разделы курса «Алгебра и теория чисел», как элементарная теория чисел, теория сравнений, цепные и непрерывные дроби, *p*-адические числа. Предназначено для студентов института радиоэлектроники и информационных технологий – РТФ.

Библиогр.: 8 назв.

УДК 511+512(075.8)
ББК 22.13я73+22.14я73

ISBN 978-5-7996-1193-4 (ч. 1)
ISBN 978-5-7996-1166-8

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Данное пособие базируется на лекциях, которые читались первым автором на радиотехническом факультете, сейчас ИРИТ–РтФ, студентам специальности МОАИС (математическое обеспечение и администрирование информационных систем) в течение ряда лет. В предлагаемой читателям первой части этого пособия рассматриваются элементарная теория чисел, теория сравнений, цепные и непрерывные дроби и немного теории p-адических чисел. Почти все теоремы приведены с доказательствами, разобрано много примеров вычислительного характера и приведено достаточно задач для самостоятельного решения. Мы надеемся, что усвоив методы, изложенные в пособии, читатель сможет применять их в различных областях математики и информатики, а также будет готов к изучению следующих разделов теории чисел: квадратичные вычеты, первообразные корни, алгебраическая теория чисел и т. д. Пособие может быть использовано в учебном процессе студентами и преподавателями Уральского федерального университета.

ГЛАВА I. ЭЛЕМЕНТАРНАЯ ТЕОРИЯ ЧИСЕЛ

§ 1. Основные теоремы

Рациональное число – отношение целых чисел, обозначение:

$$Q=\left\{\frac{p}{q}\middle|\, p,\ q\in\mathbb{Z},\ q\neq 0\right\}.$$

Определение 1. Натуральное число, отличное от единицы, называется простым числом, если его натуральными делителями являются только единица и оно само.

Теорема Евклида. Ряд простых чисел бесконечен.

Доказательство.

Предположим, что p – самое большое простое число. Рассмотрим число n = $(1\cdot 2\cdot 3\ldots p)$ + 1, где первое слагаемое – произведение всех простых чисел. Число n должно делиться на какое-то простое число $q \leq p$. Тогда из определения n следует, что $q \mid 1$. Получили противоречие, которое доказывает теорему.

Определение 2. Если натуральное число не простое и не равно единице, то оно называется составным.

Теорема 1 (о делении с остатком). Для любых целых чисел a и b при $b\neq 0$ существует единственная пара целых чисел q и r таких, что $a=bq+r$, где $0\leq r<|b|$ (a – делимое, b – делитель, q – частное, r – остаток).

Доказательство вытекает из процесса деления уголком или проводится методом индукции.

Теорема 2 (о факторизации натуральных чисел). Любое натуральное число n $(n\geq 2)$ представимо в виде $n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\ldots p_s^{\alpha_s}$, где все p_i − простые, α_i − натуральные числа. Данное представление однозначно с точностью до порядка сомножителей. Доказательство проводится индукцией по n.

Пример. Разложить на множители число 12.

12	2
6	2
3	3
1	

$12 = 2^2 \cdot 3 = 3 \cdot 2^2$ (сомножители называются факторами).

Задачи для самостоятельного решения

1) Найти частное и остаток от деления: а) 1207 на 151; б) –425 на 3.

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

3) Разложить на множители числа 39 660 и 75 600.

4) Доказать, что 3, 5 и 7 являются единственной тройкой простых чисел-близнецов (т. е. тройкой простых чисел, составляющих арифметическую прогрессию с разностью 2).

5) Найти такое простое число p, чтобы числа $4p^2 + 1$ и $6p^2 + 1$ были простыми.

Ответы:

1а) 7 и 150; б) –142 и 1.

2) 233.

3) $39660 = 2^3 \cdot 3^2 \cdot 5 \cdot 11$, $75600 = 2^4 \cdot 3^3 \cdot 5^2 \cdot 7$.

4) рассмотрим числа p, $p + 2$ и $p + 4$ (p>3). Положим $p = 3q + 1$ ($q = 2, 4, \ldots$), тогда $p + 2$ – число составное (кратное 3). Если $p = 3q + 2$ ($q = 1, 3, \ldots$), то составным является число $p + 4$.

5) $p = 5$ (рассмотреть случаи $p = \pm 1 + 5k$, $p = \pm 2 + 5k$, $k \in \mathbb{Z}$).

§ 2. Наибольший общий делитель целых чисел (НОД)

Определение 3. Пусть a и b – целые числа. Тогда натуральное число d называется наибольшим общим делителем этих чисел (d = НОД(a, b)), если

1) d – делитель и a и b;

2) если d' – другой делитель a и b, то d' делит d ($d'|d$).

НОД находится с помощью алгоритма Евклида.

Если $b = 0$, то НОД (a, 0) = a, где $a \in \mathbb{N}$, НОД (0, 0) не определен.

Пусть $a, b \in \mathbb{Z}$ $(a, b \neq 0)$.

$a = bq_1 + r_1,\ 0 \le r_1 < |b|,$

$b = r_1 q_2 + r_2,\ 0 \le r_2 < r_1,$

$r_1 = r_2 q_3 + r_3,\ 0 \le r_3 < r_2,$

…

$r_{s-2} = r_{s-1} q_s + r_s,\ 0 \le r_s < r_{s-1},$

$r_{s-1} = r_s q_{s+1} + r_{s+1},\ 0 \le r_{s+1} < r_s,$

$|b| > r_1 > r_2 > r_3 > \ldots$ Так как r_i – натуральные числа, то процесс конечен и на некотором шаге получим $r_s = r_{s+1} q_{s+2}$.

Теорема 3. $r_{s+1} = \text{НОД}(a,b)$.

Доказательство.

То, что r_{s+1} делит a и b, устанавливается из данной цепочки равенств рассуждением снизу вверх: $r_{s+1} | r_s$, откуда из второго равенства снизу вытекает, что $r_{s+1} | r_{s-1}$, далее, поднимаясь выше, получим $r_{s+1} | r_{s-2}$ и т. д. В конце этого подъема получим $r_{s+1} | b$, затем – $r_{s+1} | a$. Пусть теперь $k | a$, $k | b$. Тогда, рассуждая по цепочке сверху вниз, имеем $k | r_1$, из второго равенства $k | r_2$ и т. д. В итоге получим $k | r_{s+1}$.

Теорема доказана.

Пример. Найти НОД чисел $a = 2151$, $b = 1935$.

Применяем алгоритм Евклида:

$2151 = 1935 \cdot 1 + 216,$

$1935 = 216 \cdot 8 + 207,$

$216 = 207 \cdot 1 + 9,$

$207 = 9 \cdot 23,$

НОД(2151, 1935) = 9.

Теорема 4. Пусть d = НОД (a, b). Тогда существуют такие целые числа u и ν, что $au + b\nu = d$.

Доказательство.

Используем снова равенства в алгоритме Евклида сверху вниз: $r_1 = a - bq_1 = au_1 + b\nu_1$, где $u_1 = 1, \nu_1 = -q_1$. Из второго равенства вытекает, что $r_2 = b - r_1 q_2 = b - (au_1 + b\nu_1) q_2 = au_2 + b\nu_2$ для некоторых целых u_2, ν_2. Продолжая этот процесс, доходим до предпоследнего равенства в данном алгоритме: $r_{s+1} = (au_{s-1} + b\nu_{s-1}) - (au_s + b\nu_s) q_s = au_{s+1} + b\nu_{s+1}$ для некоторых целых u_{s+1}, ν_{s+1}.

Теорема доказана.

Задачи для самостоятельного решения

1) Найти НОД чисел 420, 126, 525.

2) Доказать, что НОД двух последовательных четных чисел равен 2, а нечетных 1.

3) Найти НОД $(10n+9, n+1)$.

Ответы:

1) НОД (420, 126, 525) = 3 (по рекуррентной формуле $\text{НОД}(a_1, a_2, a_3) = \text{НОД}(\text{НОД}(a_1, a_2), a_3)$).

2) $\text{НОД}(2n, 2n+2) = 2\,\text{НОД}(n, n+1) = 2$; $\text{НОД}(2n+1, 2n+3) = 1$ (доказывается с помощью алгоритма Евклида).

3) 1.

§ 3. Взаимно простые числа

Определение 4. Два целых ненулевых числа называются взаимно простыми, если их наибольший общий делитель равен единице.

Теорема 5. Пусть a и b целые ненулевые числа. Тогда

1) a и b взаимно простые тогда и только тогда, когда существуют целые u и v такие, что $au+b\upsilon=1$;

2) если ab делится на c и a и c взаимно простые, то b делится на c;

3) если a делится на b, a делится на c и b и c взаимно просты, то a делится на bc.

Доказательство.

1) Необходимость, очевидно, вытекает из предыдущей теоремы.

Пусть теперь $au+bv=1$ и $d \in \mathbb{N}, d|a, d|b$. Тогда $d|(au+bv)=1$, т. е. $d = 1$.

2) По пункту 1 найдутся целые u, v такие, что $au+cv=1$. Умножив это равенство на b, получим $abu+cbv=b$, откуда имеем $c|b$, т. к. $c|(abu)$ по условию и $c|(cbv)$ очевидным образом.

3) Можно считать, что $a, b, c \in \mathbb{N}$.

$b = p_1^{\beta_1} \cdot p_2^{\beta_2} \ldots p_s^{\beta_s}$, $c = q_1^{\gamma_1} \cdot q_2^{\gamma_2} \ldots q_r^{\gamma_r}$; p_i, q_j – простые, $p_i \neq q_j \ \forall i, j$.

По условию и ввиду теоремы 2 $a = M \cdot p_1^{\beta'_1} \cdot p_2^{\beta'_2} \ldots p_s^{\beta'_s} \cdot q_1^{\gamma'_1} \cdot q_2^{\gamma'_2} \ldots q_r^{\gamma'_r}$, где $M \in \mathbb{N}$ и $\beta'_i \geq \beta_i, \gamma'_j \geq \gamma_j$, откуда a делится на bc.

Теорема доказана.

Задачи для самостоятельного решения

1) Найти НОД чисел $a + b$ и ab, если НОД $(a, b) = 1$.

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

Ответы:

1) НОД $(a + b, ab) = 1$.

2) пусть НОД $(a + b, a - b) = d$, тогда $a + b = d\,x$ и $a - b = dy$, откуда $2a = d(x + y)$ и $2b = d(x - y)$. Следовательно, $d\,|(2a), d\,|(2b)$. Но $(2a, 2b) = 2$, поэтому $d\,|2$ и либо $d = 1$, либо $d = 2$.

ГЛАВА II. ТЕОРИЯ СРАВНЕНИЙ

§ 4. Основные понятия

Определение 5. Пусть n – фиксированное натуральное число, a и b – целые числа. Тогда a сравнимо с b по модулю n, если $a - b$ делится на n ($a \equiv b \bmod n$).

Теорема 6. 1) $a \equiv a \bmod n \ \forall a$;

2) $a \equiv b \bmod n \Rightarrow b \equiv a \bmod n$;

3) $a \equiv b \bmod n,\ b \equiv c \bmod n \Rightarrow a \equiv c \bmod n$.

Доказательство.

1) Очевидно.

2) Следует из того, что если $(a - b)$ делится на n, то и $(b - a)$ делится на n.

3) Следует из того, что если $(a - b)$ и $(b - c)$ делятся на n, то и $(a - c) = (a - b) + (b - c)$ делится n.

Определение 6. Класс вычетов по модулю n с представителем a равен $\{b \in \mathbb{Z} \,|\, b \equiv a \bmod n\}$.

Обозначается этот класс как $\overline{a}$.

$b \equiv a \bmod n \Rightarrow b - a = n\,z \Rightarrow b = a + n\,z.$

Поэтому $\overline{a} = a + n\mathbb{Z}$.

Теорема 7 (о классах вычетов).

1) $a \in \overline{a} = a + n\mathbb{Z} \ \forall a$;

2) $b \in \overline{a} \Rightarrow \overline{b} = \overline{a}$;

3) разные классы вычетов по модулю n не пересекаются;

4) для любого класса $\overline{a}$ по модулю n $\overline{a}=\overline{r}$, где r – остаток от деления a на n.

Доказательство.

1) Очевидно.

2) $b\in\overline{a}\Rightarrow b=a+nz$ для некоторого целого $z\Rightarrow\overline{b}=a+nz+n\mathbb{Z}=$ $=a+n\mathbb{Z}=\overline{a}$.

3) $\overline{a}\cap\overline{b}\neq\varnothing\Rightarrow\exists c\in\overline{a}\cap\overline{b}\Rightarrow\overline{a}=\overline{c}=\overline{b}\Rightarrow\overline{a}=\overline{b}$.

4) $a=nq+r\Rightarrow a\in\overline{r}\Rightarrow\overline{a}=\overline{r}$ по пункту 2.

Теорема доказана.

Следствие. Множество всех классов вычетов по модулю n равно $\left\{\overline{0},\overline{1},\ ...,\ \overline{n-1}\right\}$ (состоит из n различных классов).

Множество всех классов вычетов по модулю n обозначается $\mathbb{Z}/n\mathbb{Z}$.

Определение 7. Каноническими представителями своих классов называются $0,1,\ ...,\ n-1$.

Пример. В $\mathbb{Z}/7\mathbb{Z}$ $\overline{5}=\overline{12}=\overline{-2}=\overline{40}=...$, но каноническим представителем в $\overline{5}$ является 5.

Задачи для самостоятельного решения

1) Какие из следующих сравнений являются верными: а) $1\equiv-5\bmod 6$; б) $546\equiv 0\bmod 13$; в) $2^3\equiv 1\bmod 4$; г) $3m\equiv-1\bmod m$?

2) Найти значения m, удовлетворяющие условию: а) $20\equiv 8\bmod m$; б) $3p+1\equiv p+1\bmod m$ (p – простое число).

3) Доказать, что если $3^n\equiv-1\bmod 10$, то $3^{n+4}\equiv-1\bmod 10$ ($n\in\mathbb{N}$).

Ответы:

1) – а) и б) верные, в) и г) – нет.

2) – а) m = 1, 2, 3, 4, 6, 12; б) m=1, 2, p, 2p.

3) для доказательства использовать сравнение $3^4\equiv 1\bmod 10$.

§ 5. Алгебраические действия с классами вычетов

Определение 8. Определим операции сложения и умножения в $\mathbb{Z}/n\mathbb{Z}$ следующим образом: $\overline{a}+\overline{b}=\overline{a+b}$, $\overline{a}\cdot\overline{b}=\overline{a\cdot b}$ для любых $\overline{a},\overline{b}\in\mathbb{Z}/n\mathbb{Z}$.

Докажем прежде всего корректность этого определения.

Пусть $\overline{c}=\overline{a}$, $\overline{d}=\overline{b}$. Надо доказать, что $\overline{c+d}=\overline{a+b}$, $\overline{c\cdot d}=\overline{a\cdot b}$.

Имеем $c=a+nz$, $d=b+nw$ для некоторых $z, w\in\mathbb{N}$. Тогда $c+d=(a+b)+n(z+w)\in\overline{a+b}$, откуда, по второму свойству теоремы 7 $\overline{c+d}=\overline{a+b}$. Далее, $c\cdot d=(a\cdot b)+n(z+w)+n^2zw\in\overline{a\cdot b}$, откуда $\overline{c\cdot d}=\overline{a\cdot b}$.

Корректность определения доказана.

Пример. В $\mathbb{Z}/13\mathbb{Z}$: $\overline{7}\cdot\overline{11}=\overline{77}=\overline{12}=\overline{-1}$ $(77=13\cdot5+12)$; $\overline{5^6}=\left(\overline{5^2}\right)^3=\left(\overline{25}\right)^3=\left(\overline{-1}\right)^3=\overline{-1}=\overline{12}$.

Теорема 8. $\mathbb{Z}/n\mathbb{Z}$ относительно операций сложения и умножения – коммутативное, ассоциативное кольцо с единицей (роль единицы играет $\overline{1}$, а роль нуля играет $\overline{0}$).

Доказательство.

Поскольку сложение и умножение классов вычетов сводится к сложению и умножению их представителей – целых чисел, а множество $\mathbb{Z}$ относительно обычного сложения и умножения чисел – ассоциативное коммутативное кольцо с единицей, где роль единицы играет 1, а роль кольцевого нуля играет 0, то справедливость теоремы для $\mathbb{Z}/n\mathbb{Z}$ становится ясной.

Теорема доказана.

Теорема 9. Пусть $n>1$. Тогда $\mathbb{Z}/n\mathbb{Z}$ – поле $\Leftrightarrow n$ – простое число.

Доказательство.

Необходимость. Предположим противное: $n = pq$, $1 < p < n$, $1 < q < n$. Тогда $\overline{pq}=\overline{n}=\overline{0}$, причем $\overline{p}\neq\overline{0}$, $\overline{q}\neq\overline{0}$, т. е. $\overline{p}$ и $\overline{q}$ – делители нуля в $\mathbb{Z}/n\mathbb{Z}$. Но в поле не может быть делителей нуля. Полученное противоречие доказывает требуемое.

Достаточность.

Пусть n – простое число, $\overline{a}\in\mathbb{Z}/n\mathbb{Z}$, $\overline{a}\neq\overline{0}$. Тогда $\overline{a}=\overline{j}$, где $1\le j\le n-1$, и т. к. n – простое, то j взаимно просто с n. По пункту 1 теоремы 5 найдутся целые x и y такие, что $jx+ny=1$. Тогда в $\mathbb{Z}/n\mathbb{Z}$ имеем: $\overline{j}\,\overline{x}+\overline{n}\,\overline{y}=\overline{1}$ и, т. к. $\overline{n}=\overline{0}$, то $\overline{j}\,\overline{x}=\overline{1}$. Этим мы доказали, что в $\mathbb{Z}/n\mathbb{Z}$ любой не нулевой класс имеет обратный. Следовательно, $\mathbb{Z}/n\mathbb{Z}$ – поле.

Теорема доказана.

$\mathbb{Z}/2\mathbb{Z}=\left\{\overline{0},\overline{1}\right\}$;

$\mathbb{Z}/3\mathbb{Z}=\left\{\overline{0},\overline{1},\overline{2}\right\}$;

…

$\mathbb{Z}/p\mathbb{Z}=\{\overline{0},\overline{1},...,\overline{p-1}\}$.

$\mathbb{Z}/p\mathbb{Z}=GF(p)=F_p$ называется полем Галуа порядка p.

Пример.

$\mathbb{Z}/3\mathbb{Z}$ имеет следующие таблицы Кэли для сложения и умножения:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

$\overline{1}+\overline{2}=\overline{3}=\overline{0}$, $\overline{2}+\overline{2}=\overline{4}=\overline{1}$, $\overline{2}\cdot\overline{2}=\overline{4}=\overline{1}$. Заметим, что в вычислениях в $\mathbb{Z}/3\mathbb{Z}$ черточки над представителями классов можно не писать и считать, что $\mathbb{Z}/3\mathbb{Z}=\{0,1,2\}$ или $\mathbb{Z}/3\mathbb{Z}=\{0,1,-1\}$.

Аналогично, $\mathbb{Z}/2\mathbb{Z}=\{0,1\}$. Так что $\mathbb{Z}/2\mathbb{Z}$ имеет следующие таблицы Кэли:

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

Задачи для самостоятельного решения

1) Указать все классы вычетов: а) взаимно простых с модулем 10; б) имеющих с модулем 10 НОД, равный 2; в) имеющих с модулем 10 НОД, равный 5; г) имеющих с модулем 10 НОД, равный 10.

2) Составить таблицы Кэли для $\mathbb{Z}/4\mathbb{Z}$.

Ответы к задаче 1а) $\overline{1}, \overline{3}, \overline{7}, \overline{9}$; 1б) $\overline{2}, \overline{4}, \overline{6}, \overline{8}$; 1в) $\overline{5}$; 1г) $\overline{10}$.

§ 6. Обратимые элементы в $\mathbb{Z}/n\mathbb{Z}$

Определение 9. Пусть $\overline{a}\in\mathbb{Z}/n\mathbb{Z}$. Тогда $\overline{b}$ обратный к $\overline{a}$, если $\overline{a}\cdot\overline{b}=\overline{1}$.

Определение 10. $\bar{a}$ обратим, если $\bar{a}$ имеет обратный класс.

Множество всех обратимых классов в $\mathbb{Z}/n\mathbb{Z}$ обозначается $(\mathbb{Z}/n\mathbb{Z})^*$.

Теорема 10.

1) Если $\bar{a}$ обратим в $\mathbb{Z}/n\mathbb{Z}$, то обратный к $\bar{a}$ определяется однозначно;

2) $\bar{a}$ обратим в $\mathbb{Z}/n\mathbb{Z}$ тогда и только тогда, когда a взаимно просто с n;

3) $(\mathbb{Z}/n\mathbb{Z})^*$ – группа относительно умножения классов.

Доказательство.

1) Пусть $\bar{b}, \bar{c}$ обратные к $\bar{a}$ в $\mathbb{Z}/n\mathbb{Z}$, тогда $\bar{a}\cdot\bar{b}=\bar{a}\cdot\bar{c}=\bar{1} \Rightarrow \bar{c}=(\bar{b}\cdot\bar{a})\bar{c}=\bar{b}(\bar{a}\cdot\bar{c})=\bar{b}$. Пункт 1 доказан. В дальнейшем обратный класс к $\bar{a}$ будем обозначать $\bar{a}^{-1}$.

2.1) Пусть $\bar{a}$ обратим. Тогда существует $\bar{b}$ такой, что $\bar{a}\cdot\bar{b}=\bar{1}$, т. е. $\overline{a\cdot b}=\bar{1}$, значит $a\cdot b\equiv 1 \bmod n$ или $a\cdot b=1+n\cdot z$ для некоторого $z\in\mathbb{Z}$. Пусть $d|a$ и $d|n$. Тогда $d|1 \Rightarrow d=1 \Rightarrow$ a и n взаимно просты.

2.2) Пусть a взаимно просто с n. Тогда существуют целые u и v такие, что $au+nv=1$. Следовательно, $\overline{au+nv}=\bar{1}$ в $\mathbb{Z}/n\mathbb{Z}$; $\bar{a}\bar{u}+\bar{n}\bar{v}=\bar{1}$, откуда $\bar{a}\bar{u}=\bar{1}$, т. е. $\bar{a}$ обратим в $\mathbb{Z}/n\mathbb{Z}$.

3) Пусть $\bar{a}\in(\mathbb{Z}/n\mathbb{Z})^*$, $\bar{b}\in(\mathbb{Z}/n\mathbb{Z})^*$. Требуется доказать, что $\bar{a}\cdot\bar{b}\in(\mathbb{Z}/n\mathbb{Z})^*$, $\bar{1}\in(\mathbb{Z}/n\mathbb{Z})^*$, $\bar{a}^{-1}\in(\mathbb{Z}/n\mathbb{Z})^*$.

Так как $\bar{a}\in(\mathbb{Z}/n\mathbb{Z})^*$, $\bar{b}\in(\mathbb{Z}/n\mathbb{Z})^*$, то a и b взаимно просты с n, а значит, и ab взаимно просто с n, откуда $\bar{a}\cdot\bar{b}=\overline{a\cdot b}\in(\mathbb{Z}/n\mathbb{Z})^*$.

$\bar{1}\in(\mathbb{Z}/n\mathbb{Z})^*$, т. к. $\bar{1}^{-1}=\bar{1}$.

$\bar{a}\cdot\bar{a}^{-1}=\bar{1}$, следовательно, $\bar{a}$ обратный к $\bar{a}^{-1}$, т. е. $\bar{a}^{-1}\in(\mathbb{Z}/n\mathbb{Z})^*$.

Теорема доказана.

Определение 11. $(\mathbb{Z}/n\mathbb{Z})^*$ называется мультипликативной группой кольца вычетов $\mathbb{Z}/n\mathbb{Z}$.

Если p простое, то $(\mathbb{Z}/p\mathbb{Z})^*=\{\bar{1},\bar{2},\ ...,\ \overline{p-1}\}$ и $\left|(\mathbb{Z}/n\mathbb{Z})^*\right|=p-1$.

Теорема 11.

1) Если a взаимно просто с n, то в $\mathbb{Z}/n\mathbb{Z}$ $\bar{a}\cdot\bar{x}=\bar{a}\cdot\bar{y}\Rightarrow\bar{x}=\bar{y}$.

2) Уравнение $\bar{a}\cdot\bar{x}=\bar{b}$ при a и n взаимно простых в $\mathbb{Z}/n\mathbb{Z}$ всегда имеет единственное решение ($\bar{x}$ – неизвестное).

Доказательство.

1) По теореме 10 существует $\bar{a}^{-1}$, умножив обе части исходного равенства на $\bar{a}^{-1}$, получим

$$\bar{a}^{-1}(\bar{a}\cdot\bar{x})=\bar{a}^{-1}(\bar{a}\cdot\bar{y})\Rightarrow(\bar{a}^{-1}\cdot\bar{a})\bar{x}=(\bar{a}^{-1}\cdot\bar{a})\bar{y}\Rightarrow\bar{1}\cdot\bar{x}=\bar{1}\cdot\bar{y}\Rightarrow\bar{x}=\bar{y}.$$

2) Очевидно, что $\bar{a}^{-1}\cdot\bar{b}$ решение уравнения $\bar{a}\cdot\bar{x}=\bar{b}$:

$$\bar{a}(\bar{a}^{-1}\cdot\bar{b})=(\bar{a}\cdot\bar{a}^{-1})\bar{b}=\bar{1}\cdot\bar{b}=\bar{b}.$$

Единственность $\begin{cases}\bar{a}\cdot\bar{x}_1=\bar{b},\\ \bar{a}\cdot\bar{x}_2=\bar{b},\end{cases}\Rightarrow\bar{x}_1=\bar{x}_2$ в силу пункта 1.

Теорема доказана.

Теорема 11 используется для решения линейного диофантова уравнения $ax+by=1$, где x, y – неизвестные (a, b, x, y – целые числа).

Пример. $13x+17y=3$ – линейное диофантово уравнение.

Перейдем к классам вычетов по модулю 13: $\overline{13x+17y}=\bar{3}$ в $\mathbb{Z}/13\mathbb{Z}$; $\bar{13}\,\bar{x}+\bar{17}\,\bar{y}=\bar{3}\Rightarrow\bar{17}\,\bar{y}=\bar{3}\Rightarrow\bar{4}\,\bar{y}=\bar{3}$.

$\bar{y}=\bar{4}$ (решение находим подбором) $\Rightarrow y=4+13k$, $k\in\mathbb{Z}$;

$13x+17(4+13k)=3$; $13x=3-68-17\cdot13k$; $x=-5-17k$.

Ответ:

$$\begin{cases}x=-5-17k,\\ y=4+13k,\quad k\in\mathbb{Z}.\end{cases}$$

Задачи для самостоятельного решения

Решить уравнения в целых числах 1) $9x-23y=10$; 2) $13x-19y=9$; 3) $9x+13y=-5$.

Ответ:

1) $\begin{cases}x=-4+23k,\\ y=-2+9k,\quad k\in\mathbb{Z}.\end{cases}$

2) $\begin{cases} x=8+19k; \\ y=5+13k; \end{cases} k\in\mathbb{Z}.$

3) $\begin{cases} x=-2-13k; \\ y=1+9k; \end{cases} k\in\mathbb{Z}.$

§ 7. Функция Эйлера и ее свойства

Определение 12. Пусть n – натуральное число. Тогда $\varphi(n)$ – число натуральных чисел k таких, что $1\le k\le n$ и k взаимно просто с n.

$\varphi(n)$ – называется функцией Эйлера.

$\varphi(1)=1,\ \varphi(2)=1,\ \varphi(3)=2,\ \varphi(4)=2.$

Лемма 1. Пусть p – простое, k – натуральное число.

Тогда 1) $\varphi(p)=p-1$; 2) $\varphi(p^k)=p^{k-1}(p-1)$.

Доказательство.

1) Очевидно.

2) Посчитаем, сколько в $[1, p^k]$ целых чисел, не взаимно простых с p^k, т. е. делящихся на p: $p, 2p, 3p, ..., p^{k-1}p=p^k$. В результате получим p^{k-1} чисел, не взаимно простых с p^k. Тогда $\varphi(p^k)=p^k-p^{k-1}=p^{k-1}(p-1)$.

Лемма доказана.

Примеры. $\varphi(27)=\varphi(3^3)=3^2(3-1)=18;$

$\varphi(2^k)=2^{k-1}(2-1)=2^{k-1}.$

Определение 13. Класс $\overline{a}$ в $\mathbb{Z}/n\mathbb{Z}$ называется примитивным, если a взаимно просто с n (т. е. $\overline{a}$ – обратимый).

Лемма 2. $\varphi(n)$ – число примитивных классов в $\mathbb{Z}/n\mathbb{Z}$, т. е. $\varphi(n)=\left|\left(\mathbb{Z}/n\mathbb{Z}\right)^*\right|$.

Доказательство. $\varphi(n)$ – число натуральных чисел в 1, 2, … , n, взаимно простых с n. $\mathbb{Z}/n\mathbb{Z}=\left\{\overline{0}, \overline{1}, ..., \overline{n-1}, \overline{n}\right\} \Rightarrow$ $\varphi(n)$ – число примитивных классов в $\mathbb{Z}/n\mathbb{Z}$.

Лемма доказана.

Теорема 12 (о мультипликативности функции Эйлера). Если a и b взаимно просты, то $\varphi(a\cdot b)=\varphi(a)\varphi(b)$.

Доказательство. Выпишем представителей всех классов $\mathbb{Z}/a\cdot b\mathbb{Z}$ в прямоугольную таблицу:

0	1	…	j	…	a–1
A	1+a	…	j+a	…	(a–1)+a = 2a – 1
…	…	…	…	…	…
(b–1) a	1+(b–1) a	…	j+(b–1) a	…	(a–1)+(b–1) a = ab–1

Необходимо выяснить, сколько в таблице чисел, взаимно простых с ab, т. е. и с a, и с b одновременно.

Выясним, сколько взаимно простых чисел с a. Числа в j-столбце взаимно просты с a тогда и только тогда, когда j взаимно просто с a. Таких столбцов $\varphi(a)$ штук, т. е. чисел, взаимно простых с a, в таблице $\varphi(a)b$ штук.

Рассмотрим любой столбец, где j взаимно просто с a, перейдем в нем к классам вычетов по модулю b. Докажем, что все классы вычетов в этом столбце разные. Предположим, что $\overline{j+ka}=\overline{j+la}$, $0\le k,l\le b-1$ в $\mathbb{Z}/b\mathbb{Z}$. Тогда $\bar{j}+\bar{k}\bar{a}=\bar{j}+\bar{l}\bar{a}$ и, следовательно, $\bar{k}\bar{a}=\bar{l}\bar{a}$. Так как a взаимно просто с b, то в $\mathbb{Z}/b\mathbb{Z}$ существует $\bar{a}^{-1}$. Преобразуем полученное равенство: $\left(\bar{k}\bar{a}\right)\bar{a}^{-1}=\left(\bar{l}\bar{a}\right)\bar{a}^{-1}\Rightarrow\bar{k}=\bar{l}$, причем $0\le k,l\le b-1$, следовательно, $k=l$.

Доказали, что в столбце все классы по модулю b разные. Поэтому, по определению функции Эйлера, среди чисел $j,\ j+a,\ ...,\ j+(b-1)a$ ровно $\varphi(b)$ чисел, взаимно простых с b.

В итоге получаем $\varphi(a)$ столбцов, в которых все числа взаимно просты с a и в каждом $\varphi(b)$ чисел, взаимно простых с b. Общее количество чисел, взаимно простых и с a, и с b равно $\varphi(a)\varphi(b)$.

Теорема доказана.

Пример. $\varphi(24)=\varphi(2^3)\varphi(3)=4\cdot2=8$;
$\varphi(35)=\varphi(5)\varphi(7)=4\cdot6=24$.

Теорема 13 (Эйлера). Пусть a взаимно просто с n. Тогда $a^{\varphi(n)} \equiv 1 \bmod n$.

Доказательство. Выпишем все примитивные классы по модулю n в $\mathbb{Z}/n\mathbb{Z}$: $\bar{x}_1, \bar{x}_2, ..., \bar{x}_{\varphi(n)}$ и умножим каждый на $\bar{a}$. Так как x_i и a взаимно просты с n, то класс $\bar{a}\bar{x}_i = \overline{ax_i}$ примитивен для любого i.

$\{\bar{a}\bar{x}_1, \bar{a}\bar{x}_2, ..., \bar{a}\bar{x}_{\varphi(n)}\}$ обозначим M.

Предположим, что $\overline{ax_k} = \overline{ax_l}$; a взаимно просто с n $\Rightarrow$ $\Rightarrow$ $\bar{a}^{-1}\left(\bar{a}\bar{x}_k\right) = \bar{a}^{-1}\left(\bar{a}\bar{x}_l\right) \Rightarrow \overline{x_k} = \overline{x_l}$. Доказали, что все классы в M попарно различны, т. е. множество M – это полный набор примитивных классов по модулю n. Следовательно,

$$\bar{x}_1 \cdot \bar{x}_2 ... \bar{x}_{\varphi(n)} = \overline{ax}_1 \cdot \overline{ax}_2 ... \overline{ax}_{\varphi(n)} \Rightarrow$$

$$\overline{x_1 x_2 ... x_{\varphi(n)}} = \bar{a}^{\varphi(n)} \overline{x_1 x_2 ... x_{\varphi(n)}} \Rightarrow \bar{1} = \bar{a}^{\varphi(n)} \Rightarrow 1 \equiv a^{\varphi(n)} \bmod n.$$

Теорема доказана.

Следствие (малая теорема Ферма). Если p – простое число, a не делится на p, то $a^{p-1} \equiv 1 \bmod p$.

Доказательство. Следует из теоремы Эйлера, так как $\varphi(p) = p - 1$.

Пример.

Какой остаток имеет 1380^{1945} при делении на 19?

Деля уголком 1380 на 19, получаем остаток 12, т. е. $\overline{1380} = \overline{12}$ в $\mathbb{Z}/19\mathbb{Z}$. Число 1945 делим с остатком на $\varphi(19) = 18$: $1945 = 18 \cdot 108 + 1$. Следовательно, в $\mathbb{Z}/19\mathbb{Z}$ имеем $\overline{1380^{1945}} = \overline{12}^{18 \cdot 108 + 1} = \overline{12}^{1}$, так как по теореме Ферма $\overline{12}^{18} = \bar{1}$ в $\mathbb{Z}/19\mathbb{Z}$.

Ответ: 12.

Задачи для самостоятельного решения

1) Показать, что число $13^{176} - 1$ делится на 89; 2) показать, что $(73^{12} - 1)$ делится на 105.

§ 8. Решение линейных сравнений с помощью функции Эйлера

Пусть дано сравнение $a\,x \equiv b \bmod n$ при a и n взаимно простых (x – неизвестное целое). Тогда $\bar{a}\,\bar{x} = \bar{b}$ в $\mathbb{Z}/n\mathbb{Z}$.

$\bar{a}^{-1}\bar{a}\,\bar{x} = \bar{a}^{-1}\bar{b}$;

$\bar{x} = \bar{a}^{-1}\bar{b}$;

$\bar{a}^{\varphi(n)} = \bar{1} \Rightarrow \bar{a}\cdot\bar{a}^{\varphi(n)-1} = \bar{1} \Rightarrow \ \bar{a}^{-1} = \bar{a}^{\varphi(n)-1}$.

Пример. $17\,x \equiv 38 \bmod 71$ равносильно $\overline{17}\,\bar{x} = \overline{38}$ в $\mathbb{Z}/71\mathbb{Z}$. Тогда $\bar{x} = \overline{17}^{-1}\overline{38}$; $\varphi(71) = 70$. По формуле выше

$$\overline{17}^{-1} = \overline{17}^{69} = \overline{17}^{64}\cdot\overline{17}^{4}\cdot\overline{17} = \overline{25}\cdot\overline{25}\cdot\overline{17} = \overline{-14}\cdot\overline{17} = \overline{-238} = \overline{-25}.$$

Комментарии:

$$69 = 2^6 + 2^2 + 2^0;\ \overline{17}^{2} = \overline{289} = \bar{5};\ 289 = 71\cdot 4 + 5;\ 625 = 71\cdot 8 + 57;$$

$$\overline{17}^{4} = \bar{5}^{2} = \overline{25};\ \overline{17}^{8} = \overline{25}^{2} = \overline{625} = \overline{57} = \overline{-14};\ \overline{17}^{16} = \overline{-14}^{2} = \overline{196} = \overline{54} = \overline{-17};$$

$$\overline{17}^{32} = \overline{289} = \bar{5};\ \overline{17}^{64} = \bar{5}^{2} = \overline{25};\ \overline{17}^{-1} = \overline{-25}.$$

$\bar{x} = \overline{-25}\cdot\overline{38} = \overline{-950} = \overline{-27} = \overline{44}$.

Ответ: $x = 44 + 71k$, $k \in \mathbb{Z}$.

Задачи для самостоятельного решения

Решить сравнения: а) $29x \equiv 1 \bmod 17$;

б) $21x + 5 \equiv 0 \bmod 29$; в) $19x \equiv 28 \bmod 53$.

Ответ: а) $x = 10 + 17k$, $k \in \mathbb{Z}$; б) $x = -3 + 29k$, $k \in \mathbb{Z}$;

в) $x = 11 + 53k$, $k \in \mathbb{Z}$.

§ 9. Китайская теорема об остатках

Рассмотрим систему сравнений $\begin{cases} x \equiv x_1 \bmod n_1; \\ x \equiv x_2 \bmod n_2; \\ \ldots \\ x \equiv x_k \bmod n_k, \end{cases}$ (1)

где x − неизвестное целое, числа n_i попарно взаимно простые.

Аналогично систему можно рассмотреть для многочленов над полем F:

$$\begin{cases} f(x)\equiv\varphi_1(x)\bmod\psi_1(x); \\ f(x)\equiv\varphi_2(x)\bmod\psi_2(x); \\ \ldots \\ f(x)\equiv\varphi_k(x)\bmod\psi_k(x). \end{cases}$$

($\psi_i(x),\psi_j(x)$ − взаимно простые при $i\neq j$ над полем F).

По аналогии с теорией чисел $f(x)\equiv\varphi(x)\bmod\psi(x)$ тогда и только тогда, когда $f(x)-\varphi(x)$ делится на $\psi(x)$.

Пусть $N=n_1\cdot n_2\ldots n_k,\ m_j=\dfrac{N}{n_j}=n_1\ldots n_{j-1}\cdot n_{j+1}\ldots n_k$.

Например, $n_1=2, n_2=3, n_3=5$. Тогда $N=30,\ m_1=15,\ m_2=10,\ m_3=6$.

Теорема 14. Пусть x_0 − любое частное решение системы (1). Тогда все числа из $x_0+N\mathbb{Z}$ также частные решения системы (1).

Доказательство. $\hat{x}\in x_0+N\mathbb{Z}\ \Rightarrow\ \hat{x}\equiv x_0\bmod N\ \Rightarrow\ \hat{x}\equiv x_0\bmod n_j$ $\forall j=\overline{1,k}$, т. к. $N=n_1\cdot n_2\ldots n_k$. Учитывая, что $x_0\equiv x_j\bmod n_j$, в силу (1) имеем $\hat{x}\equiv x_j\bmod n_j\ \ \forall j=\overline{1,k}$. Значит, $\hat{x}$ − частное решение.

Теорема доказана.

Теорема 15. Пусть $\hat{x}$ и $\tilde{x}$ − частные решения системы (1). Тогда $\hat{x}\equiv\tilde{x}\bmod N$.

Доказательство.

$\forall j=\overline{1,k}\ \ \hat{x}\equiv x_j\bmod n_j,\ \tilde{x}\equiv x_j\bmod n_j\ \Rightarrow\ \hat{x}\equiv\tilde{x}\bmod n_j$, т. е. $\hat{x}-\tilde{x}$ делится на n_j. Так как n_j попарно взаимно простые, то по 3-му свойству взаимно простых чисел $\hat{x}-\tilde{x}$ делится на $n_1\cdot n_2\ldots n_k=N$, откуда $\hat{x}\equiv\tilde{x}\bmod N$.

Теорема доказана.

Следствие. Множество всех решений системы (1), если она совместна, представляет собой класс вычетов по модулю N, причем единственный.

Теорема 16. Обозначим y_j как любое целое число, удовлетворяющее сравнению $m_jy_j\equiv x_j\bmod n_j\ \ (j=\overline{1,k})$; y_j существует, так как m_j взаимно просто с n_j. Тогда $x_0=m_1y_1+m_2y_2+\ldots+m_ky_k$ − частное решение системы (1).

Доказательство.

Фиксируем j от 1 до k. Требуется доказать, что $x_0 \equiv x_j \bmod n_j$, т. е. $\bar{x}_0 = \bar{x}_j$ в $\mathbb{Z}/n_j\mathbb{Z}$. $\overline{x_0} = \overline{m_1 y_1} + \ldots + \overline{m_j y_j} + \ldots + \overline{m_k y_k} = \overline{x_j}$, так как в каждом $m_s y_s$ при $s \neq j$ присутствует n_j.

Теорема доказана.

Совокупность теорем 14–16 называется Китайской теоремой об остатках.

Пример. Решить систему сравнений $\begin{cases} x \equiv 3 \bmod 9; \\ x \equiv 6 \bmod 13; \\ x \equiv 1000 \bmod 17. \end{cases}$

$N = 9 \cdot 13 \cdot 17 = 1989$; $m_1 = 13 \cdot 17 = 221$; $m_2 = 9 \cdot 17 = 153$; $m_3 = 9 \cdot 13 = 117$.

$221 y_1 \equiv 3 \bmod 9$; $\quad 221 = 9 \cdot 24 + 5$;

$5 y_1 \equiv 3 \bmod 9$;

$\overline{y_1} = \overline{6} = \overline{-3}$.

$153 y_2 \equiv 6 \bmod 13$; $\quad 153 = 13 \cdot 11 + 10$;

$10 y_1 \equiv 6 \bmod 13$;

$\overline{y_2} = \overline{-2}$.

$117 y_3 \equiv 1000 \bmod 17$; $\quad 117 = 17 \cdot 6 - 15$;

$-2 y_3 \equiv 14 \bmod 17$;

$\overline{y_3} = \overline{-7}$.

$x_0 = 221(-3) + 153(-2) + 117(-7) = -663 - 306 - 819 = -1788$;

$-1788 \equiv 3 \bmod 9$; $\quad -1788 \equiv 6 \bmod 13$; $\quad -1788 \equiv 1000 \bmod 17$.

$x = -1788 + 1989k = 201 + 1989k$, $k \in \mathbb{Z}$.

Ответ: $x = 201 + 1989k$, $k \in \mathbb{Z}$.

Задачи для самостоятельного решения

1) Решить систему сравнений $\begin{cases} x \equiv 3 \bmod 7; \\ x \equiv 2 \bmod 11; \\ x \equiv 5 \bmod 13. \end{cases}$

2) Найти числа, которые при делении на 7, 13, 17 дают в остатке соответственно 4, 9 и 1.

Ответы:

1) $x = 486 + 1001k$, $k \in \mathbb{Z}$; 2) $x = 256 + 1547k$, $k \in \mathbb{Z}$.

§ 10. Обобщение китайской теоремы об остатках

Теорема 17.

Система $\begin{cases} x \equiv x_1 \bmod n_1; \\ x \equiv x_2 \bmod n_2; \\ \ldots \\ x \equiv x_k \bmod n_k \end{cases}$

совместна тогда и только тогда, когда $\forall i, j \;\; x_i \equiv x_j \bmod \text{НОД}(n_i, n_j)$.

Теорема 18.

Если система $\begin{cases} x \equiv x_1 \bmod n_1; \\ x \equiv x_2 \bmod n_2; \\ \ldots \\ x \equiv x_k \bmod n_k \end{cases}$

совместна, то при любом частном решении x_0 ее общее решение имеет вид $x = x_0 + N\mathbb{Z}$, где $N = \text{НОК}(n_1, n_2, \ldots, n_k)$.

Пример. Решить систему сравнений $\begin{cases} x \equiv 1 \bmod 6; \\ x \equiv 4 \bmod 21; \\ x \equiv 7 \bmod 9. \end{cases}$

Из первого сравнения получаем $x=1+6k$, $k \in \mathbb{Z}$; из второго сравнения имеем $1+6k \equiv 4 \bmod 21$, т. е. $6k \equiv 3 \bmod 21$, откуда $2k \equiv 1 \bmod 7$ и, следовательно, $k = 4+7m$, $m \in \mathbb{Z}$. Тогда $x=1+6(4+7m)=25+42m$. Подставим полученное выражение в последнее сравнение: $25+42m \equiv 7 \bmod 9$. Получим $-2+42m \equiv -2 \bmod 9$, откуда $-2-3m \equiv -2 \bmod 9$, т. е. $-3m \equiv 0 \bmod 9$, $m \equiv 0 \bmod 3$ и $m=3l$, $l \in \mathbb{Z}$.

$6 = 2 \cdot 3, 21 = 3 \cdot 7, 9 = 3 \cdot 3 \Rightarrow \text{НОК}(6,21,9) = 2 \cdot 3^2 \cdot 7 = 126.$

Ответ: $x=25+126l$, $l \in \mathbb{Z}$.

§ 11. Примеры решения задач по теории сравнений

Пример 1. Решить уравнение $17x-28y=1$ в целых числах.

Решение.

$\overline{17x-28y} = \overline{1}$ в $\mathbb{Z}/17\mathbb{Z}$.

$-\overline{28}\,\overline{y} = \overline{1}$; $\overline{28}\,\overline{y} = -\overline{1}$; $11\overline{y} = -\overline{1}$; $\overline{y} = \overline{3} \Rightarrow y = 3+17k$.

$17x-28(3+17k)=1$; $17x=85+28\cdot 17k$; $x=5+28k$.

Ответ: $\begin{cases} x=5+28k; \\ y=3+17k; \end{cases}$ $k\in\mathbb{Z}$.

Пример 2. Решить уравнение $13x+21y=10$ в целых числах.

Решение.

$\overline{13x+21y}=\overline{10}$ в $\mathbb{Z}/13\mathbb{Z}$.

$\overline{21}\,\overline{y}=\overline{10}$; $\overline{8}\,\overline{y}=\overline{10}$; $\overline{y}=-\overline{2} \Rightarrow y=-2+13k$.

$x=4-21k$.

Ответ: $\begin{cases} x=4-21k; \\ y=-2+13k; \end{cases}$ $k\in\mathbb{Z}$.

Пример 3. Решить уравнение $17x+13y+19z=1$ в целых числах.

Решение.

$\overline{17x+13y+19z}=\overline{1}$ в $\mathbb{Z}/13\mathbb{Z}$.

$\overline{17x+19z}=\overline{1}$; $\overline{4x}=\overline{1-6z}$.

$\overline{4}\,\overline{x}=\overline{1-6z} \Rightarrow x=\overline{4^{-1}}\,\overline{1-6z}=\overline{-3}\,\overline{1-6z}=\overline{-3+18z}$.

$\overline{4}\,\overline{4^{-1}}=\overline{1}$; $\overline{4^{-1}}=\overline{-3}$.

$x=18z-3+3k$, $k\in\mathbb{Z}$.

$17(18z-3+13k)+13y+19z=1$.

$13y=-19z-17\cdot 18z+52-17\cdot 13k$.

$13y=-325z+52-17\cdot 13k$

Ответ: $\begin{cases} x=18z-3+13k; \\ y=-25z+4-17k; \end{cases}$ $k,z\in\mathbb{Z}$.

Пример 4. Решить уравнение $11x-17y+15z=7$ в целых числах.

Решение.

$\overline{11x-17y+15z}=\overline{7}$ в $\mathbb{Z}/11\mathbb{Z}$.

$\overline{5y+4z}=\overline{7}$; $\overline{6y}=\overline{4z+4}$; $\overline{y}=\left(\overline{6}\right)^{-1}\overline{4z+4}$.

$\overline{6}\left(\overline{6}\right)^{-1}=\overline{1}$ в $\mathbb{Z}/11\mathbb{Z} \Rightarrow \left(\overline{6}\right)^{-1}=\overline{2}$.

$y=8z+8+11k$.

$11x-17(8z+8+11k)+15z=7$;

$11x = 143 + 121z + 17 \cdot 11k$;

$x = 13 + 11z + 17k$.

Ответ: $\begin{cases} x = 13 + 11z + 17k; \\ y = 8z + 8 + 11k; \end{cases} \quad k, z \in \mathbb{Z}.$

Пример 5. Найти остаток при делении 1825^{2199} на 23.

Решение.

$1825 = 23 \cdot 79 + 8$.

В $\mathbb{Z}/23\mathbb{Z}$ $\overline{1825^{2199}} = \left(\bar{8}\right)^{\overline{2199}}$; $\varphi(23) = 22$, так как 23 – простое число, $\left(\bar{8}\right)^{22} = \bar{1}$; $2199 = 22 \cdot 99 + 21$.

Тогда $\left(\bar{8}\right)^{\overline{2199}} = \left(\bar{8}\right)^{22 \cdot 99 + 21} = \left(\bar{1}\right)^{99} \cdot \left(\bar{8}\right)^{21} = \left(\bar{8}\right)^{21} = \left(\bar{8}\right)^{-1} = \bar{3}$.

($\bar{8}^{21} \cdot \bar{8} = \bar{1} \Rightarrow \bar{8}^{21} = \left(\bar{8}\right)^{-1}$ в $\mathbb{Z}/23\mathbb{Z}$).

Ответ: остаток равен 3.

Пример 6. Найти остаток при делении 2102^{3076} на 27.

Решение.

$27 = 3^3$, $\varphi(27) = 3^2(3-1) = 18$, $2102 = 27 \cdot 77 + 23$, $3076 = 18 \cdot 170 + 16$.

$\overline{2102^{3076}} = \left(\overline{23}\right)^{\overline{3076}} = \overline{23^{16}} = \overline{-4^{16}} = \overline{7^2} = \overline{49} = \overline{22}$

($\overline{-4^2} = \overline{16}$; $\overline{-4^4} = \overline{256} = \overline{-14}$; $\overline{-4^8} = \overline{196} = \overline{7}$).

Ответ: остаток равен 22.

Пример 7. Решить линейное сравнение с помощью функции Эйлера: $27x \equiv 32 \bmod 56$.

Решение.

27 и 56 – взаимно простые, следовательно, решение есть.

$\overline{27x} = \overline{32}$ в $\mathbb{Z}/56\mathbb{Z}$; $\bar{x} = \left(\overline{27}\right)^{-1} \overline{32}$.

$\left(\overline{27}\right)^{-1} = \left(\overline{27}\right)^{\varphi(56)-1} = \left(\overline{27}\right)^{23} = \left(\overline{27}\right)^{16+4+2+1} = \overline{27}$;

($\varphi(56) = \varphi(7)\varphi(8) = 6 \cdot 4 = 24$, $\left(\overline{27}\right)^2 = \overline{729} = \bar{1}$, $\left(\overline{27}\right)^4 = \left(\overline{27}\right)^{16} = \bar{1}$).

$\bar{x} = \overline{27} \cdot \overline{32} = \overline{864} = \overline{24}$.

Ответ: $x = 24 + 56k$, $k \in \mathbb{Z}$.

Пример 8. Решить линейное сравнение с помощью функции Эйлера: $41x \equiv 29 \bmod 63$.

Решение.

41 и 63 – взаимно простые, следовательно, решение есть.

$\overline{41x}=\overline{29}$ в $\mathbb{Z}/63\mathbb{Z}$; $\bar{x}=\left(\overline{41}\right)^{-1}\overline{29}$;

$\left(\overline{41}\right)^{-1}=\left(\overline{41}\right)^{\varphi(63)-1}=\left(\overline{41}\right)^{35}=\left(\overline{41}\right)^{32+2+1}$;

$(\varphi(63)=\varphi(7)\varphi(9)=6\cdot 6=36)$;

$\left(\overline{41}\right)^{2}=\overline{1681}=\overline{43}=\overline{-20}$, $\left(\overline{41}\right)^{4}=\left(\overline{-20}\right)^{2}=\overline{400}=\overline{22}$;

$\left(\overline{41}\right)^{8}=\left(\overline{22}\right)^{2}=\overline{484}=\overline{43}=\overline{-20}$;

$\left(\overline{41}\right)^{16}=\left(\overline{-20}\right)^{2}=\overline{22}$;

$\left(\overline{41}\right)^{32}=\left(\overline{22}\right)^{2}=\overline{-20}$;

$\left(\overline{41}\right)^{32+2+1}=\overline{-20}\cdot\overline{-20}\cdot\overline{41}=\overline{400}\cdot\overline{41}=\overline{22}\cdot\overline{41}=\overline{902}=\overline{20}$;

$\bar{x}=\overline{20}\cdot\overline{29}=\overline{580}=\overline{13}$.

Ответ: $x=13+63k,\ k\in\mathbb{Z}$.

Пример 9. Решить систему сравнений:

$$\begin{cases} 7x+9y\equiv 1 \bmod 13 \\ 5x-7y\equiv 2 \bmod 11. \end{cases}$$

Решение.

$5x-7y\equiv 2 \bmod 11 \Leftrightarrow \overline{5x-7y}=\overline{2}$ в $\mathbb{Z}/11\,\mathbb{Z} \Leftrightarrow \overline{5}\,\overline{x}=\overline{2+7y} \Leftrightarrow$

$\Leftrightarrow \bar{x}=\overline{-4-14y} \Leftrightarrow \bar{x}=\overline{-4-3y} \Leftrightarrow x=-4-3y+11k,\ k\in\mathbb{Z}$.

Подставим полученное выражение для x в первое сравнение системы: $7(-4-3y+11k)+9y\equiv 1 \bmod 13 \Leftrightarrow$

$\Leftrightarrow -28-12y+77k\equiv 1 \bmod 13 \Leftrightarrow -2+y-k\equiv 1 \bmod 13 \Leftrightarrow k$ имеет вид $-3+y+13m,\ m\in\mathbb{Z}$. Тогда

$$x=-4-3y+11(-3+y+13m)=-37+8y+143m,\ m\in\mathbb{Z}.$$

Ответ: $x=-37+8y+143m,\ y,\ m\in\mathbb{Z}$.

Пример 10. Решить систему уравнений в целых числах $\begin{cases}23x+17y+13z=27;\\15x-11y-9z=13.\end{cases}$

Решение.

Подбором находим частное решение (1, 1, –1). Далее находим направляющий вектор прямой, заданной данной системой уравнений: $\bar{q}=\begin{vmatrix}\bar{i} & \bar{j} & \bar{k}\\23 & 17 & 13\\15 & -11 & -9\end{vmatrix}=(10;\,402;\,-508)$. Тогда параметрические уравнения прямой имеют вид: $x=1-5t$, $y=1+201t$, $z=-1-254t$. Если $t=\frac{p}{q}$, $q>0$ и дробь $\frac{p}{q}$ несократима, то $q|5$, $q|201$, $q|(-254)$, откуда $q=1$, т. е. $t\in\mathbb{Z}$.

Ответ: $x=1-5t$, $y=1+201t$, $z=-1-254t$, $t\in\mathbb{Z}$.

Пример 11. Какие остатки может иметь выражение $2013n^{2012}-2012n^{2013}$ при делении на 7 ($n\in\mathbb{Z}$)?

Решение.

Пусть $f(n)=2013n^{2012}-2012n^{2013}$. Тогда в $\mathbb{Z}/7\mathbb{Z}$ $\overline{f(n)}=\bar{4}\bar{n}^2-\bar{3}\bar{n}^3$ при n взаимно простом с 7 (учитывалось, что $\bar{n}^6=\bar{1}$). Тогда $\overline{f(1)}=\bar{1}$, $\overline{f(2)}=\bar{6}$, $\overline{f(3)}=\bar{4}$, $\overline{f(-3)}=\bar{5}$, $\overline{f(-2)}=\bar{5}$, $\overline{f(-1)}=\bar{0}$. При n кратном 7 $\overline{f(n)}=\bar{0}$.

Ответ: остатки могут быть 0, 1, 3, 4, 5, 6.

Пример 12. Найти остаток при делении 1404^{2012} на 23.

Решение.

$\overline{1404^{2012}}=\left(\bar{1}\right)^{2012}=\bar{1}$

Ответ: остаток равен 1.

Пример 13. Найти остаток при делении 2012^{1404} на 15.

Решение.

$\varphi(15)=\varphi(3)\varphi(5)=2\cdot4=8$, $1404 = 8\cdot175 + 4$.

$\overline{2012^{1404}}=\left(\bar{2}\right)^{\overline{1404}}=\overline{2^4}=\overline{16}=\bar{1}$.

Ответ: остаток равен 1.

Теорема 19 (делимость на 11 и на 9).

Пусть $A = a_n\, a_{n-1}\, \ldots\, a_0$. Если r – остаток от деления A на 11, то $\bar{r} = \overline{a_0 - a_1 + a_2 - \ldots + (-1)^n a_n}$ в $\mathbb{Z}/11\mathbb{Z}$. Если t остаток от деления на 9, то $\bar{t} = \overline{a_0 + a_1 + a_2 + \ldots + a_n}$ в $\mathbb{Z}/9\mathbb{Z}$.

Доказательство.

В $\mathbb{Z}/11\mathbb{Z}$ $\begin{cases} \bar{1} = \bar{1}; \\ \overline{10} = \overline{-1}; \\ \overline{10}^2 = \bar{1}; \\ \ldots \\ \overline{10}^k = \overline{(-1)}^k. \end{cases}$

$A = a_0 + 10\, a_1 + 10^2\, a_2 + \ldots + 10^n\, a_n.$

$$\bar{r} = \overline{A} = \overline{a_0} + \overline{10}\overline{a_1} + \overline{10}^2\overline{a_2} + \ldots + \overline{10}^n\overline{a_n} =$$

$$= a_0 - \overline{a_1} + \overline{a_2} - \ldots + \overline{(-1)^n a_n} = \overline{a_0 - a_1 + a_2 - \ldots + (-1)^n a_n}.$$

Первая часть теоремы доказана. Вторая часть теоремы доказывается аналогично.

Пример 14. Найти остатки при делении числа 2856897 на 11 и на 9.

Решение.

$7+9+8+6+5+8+2 \equiv 36 \bmod 9$, т. е. данное число делится на 9 без остатка. $7-9+8-6+5-8+2 = -1 \equiv 10 \bmod 11$, т. е. остаток при делении на 11 равен 10.

Пример 15. Решить систему сравнений $\begin{cases} x \equiv 3000 \bmod 11; \\ x \equiv 22 \bmod 29; \\ x \equiv 7 \bmod 9. \end{cases}$

Решение.

$N = 11 \cdot 29 \cdot 9 = 2871;\ m_1 = 29 \cdot 9 = 261;$

$m_2 = 11 \cdot 9 = 99;\ m_3 = 11 \cdot 29 = 319.$

$216 y_1 \equiv 8 \bmod 11;$ $\quad 261 = 11 \cdot 23 + 6;$

$8 y_1 \equiv 8 \bmod 11;$

$y_1 = 1.$

$99 y_2 \equiv 22 \bmod 29;$ $\quad 99 = 29 \cdot 3 + 12;$

$12 y_1 \equiv 22 \bmod 29;$

$y_2 = -3.$

$319y_3 \equiv 7 \bmod 9$; $319 = 9 \cdot 35 + 4$;

$4y_3 \equiv 7 \bmod 9$;

$y_3 = 4$.

$m_1y_1 + m_2y_2 + m_3y_3 = 261 \cdot 1 + 99(-3) + 319 \cdot 4 = 261 - 297 + 1276 = 1240$.

Ответ: $x = 1240 + 2871k,\ k \in \mathbb{Z}$.

Пример 16. Решить систему сравнений $\begin{cases} x \equiv 3 \bmod 6; \\ x \equiv 15 \bmod 21; \\ x \equiv 1 \bmod 35. \end{cases}$

Решение.

$x = 3 + 6k \equiv 15 \bmod 21$; $1 + 2k \equiv 5 \bmod 7$; $2k \equiv 4 \bmod 7$; $\overline{2k} = \overline{4}$ в $\mathbb{Z}/7\mathbb{Z}$. $\overline{k} = \overline{2} \Rightarrow k = 2 + 7m$.

$x = 3 + 6(2 + 7m) = 15 + 42m \equiv 1 \bmod 35$; $42m \equiv -14 \bmod 35$; $6m \equiv -2 \bmod 5$.

$\overline{m} = \overline{-2}$ в $\mathbb{Z}/5\mathbb{Z}$; $m = -2 + 5l$.

$x = 15 + 42(-2 + 5l) = -69 + 210l,\ l \in \mathbb{Z}$.

Ответ: $x = -69 + 210l,\ l \in \mathbb{Z}$.

Задачи для самостоятельного решения

1) Решить уравнения в целых числах: а) $17x + 23y = 1$; б) $118x - 37y = 2$; в) $13x + 16y + 19z = 1$; г) $23x - 11y + 15z = 2$.

2) Найти остатки при делении указанных чисел x на указанные числа y: а) $x = 1941^{1945}$; $y = 17$; б) $x = 1380^{1917}$; $y = 23$.

3) Решить сравнение с помощью функции Эйлера: а) $37x \equiv 24 \bmod 61$; б) $34x \equiv 13 \bmod 59$.

4) Решить системы сравнений:

а) $\begin{cases} x \equiv 100 \bmod 13; \\ x \equiv 200 \bmod 17; \\ x \equiv 300 \bmod 19. \end{cases}$ б) $\begin{cases} x \equiv -8 \bmod 15; \\ x \equiv 13 \bmod 23; \\ x \equiv 11 \bmod 17; \\ x \equiv 2 \bmod 9. \end{cases}$

5) Решить системы сравнений:

а) $\begin{cases} 5x - 8y \equiv 3 \bmod 17; \\ 6x + 19y \equiv 13 \bmod 23. \end{cases}$ б) $\begin{cases} 12x + 1000y \equiv 13 \bmod 21; \\ 17x - 9y \equiv 5 \bmod 13. \end{cases}$

ГЛАВА III. ЦЕПНЫЕ И НЕПРЕРЫВНЫЕ ДРОБИ

§ 12. Разложение рационального числа в цепную дробь

Определение 13. Цепная дробь – это дробь вида

$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\ddots\cfrac{1}{a_{s-1}+\cfrac{1}{a_s}}}},$$

где $a_0\in\mathbb{Z}, a_i\in\mathbb{N}$ при $1\le i\le s-1$, $a_s\in\mathbb{N}$ и $a_s\ge 2$.

Данное выражение без ограничений – обобщенная цепная дробь. Краткая запись – $[a_0, a_1, \dots, a_s]$.

Теорема 20. Любое рациональное число $\frac{P}{Q}$ $(Q>0)$ представимо в виде цепной дроби $(P, Q\in\mathbb{Z})$.

Доказательство.

Применим алгоритм Евклида к паре (P, Q).

$P=Qa_0+r_1,\ 0\le r_1<Q \Rightarrow \frac{P}{Q}=a_0+\frac{1}{Q/r_1}$;

$Q=r_1a_1+r_2,\ 0\le r_2<r_1$;

$r_1=r_2a_2+r_3,\ 0\le r_3<r_2$ и т. д. Получим

$$\frac{P}{Q}=a_0+\frac{1}{\frac{r_2}{r_1}}=a_0+\frac{1}{a_1+\frac{1}{r_1/r_2}}=a_0+\frac{1}{a_1+\frac{1}{a_2+r_3/r_2}}=$$

$$=a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{r_2/r_3}}}=\dots=a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\ddots\cfrac{1}{a_{s-1}+\cfrac{1}{a_s}}}},$$

где $r_{s-1}=r_sa_s$.

Теорема доказана.

§ 13. Подходящие дроби

Определение 14. Пусть $P/Q = [a_0, a_1, \dots, a_s]$. Тогда n-я подходящая дробь $A_n = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}$,

где $0 \le n \le s$.

Определим две последовательности P_n и Q_n рекуррентным образом по данной цепной дроби:

$P_0 = a_0$;	$Q_0 = 1$;
$P_1 = a_0 a_1 + 1$;	$Q_1 = a_1$;
$P_2 = a_2 P_1 + P_0$;	$Q_2 = a_2 Q_1 + Q_0$;
…	…
$P_n = a_n P_{n-1} + P_{n-2}$;	$Q_n = a_n Q_{n-1} + Q_{n-2}$.

Теорема 21. Для любого n ($0 \le n \le s$) n-я подходящая дробь $A_n = P_n/Q_n$.

Доказательство.

Используем принцип математической индукции.

База индукции:

$$n = 0 \Rightarrow A_0 = a_0 = \frac{a_0}{1} = \frac{P_0}{Q_0};$$

$$n = 1 \Rightarrow A_1 = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{P_1}{Q_1}.$$

Шаг индукции: предположим, что формула верна для A_n ($A_n = P_n/Q_n$), и докажем, что формула верна для A_{n+1}.

Доказательство индукции:

$$A_{n+1} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots \cfrac{1}{a_n + \cfrac{1}{a_{n+1}}}}},$$

рассмотрим $a_n + \frac{1}{a_{n+1}}$ как единое целое, тогда длина дроби равна n и можно применить формулу для A_n.

$$A_{n+1} = \frac{P_n'}{Q_n'} = \frac{P'_{n-2} + \left(a_n + \frac{1}{a_{n+1}}\right)P'_{n-1}}{Q'_{n-2} + \left(a_n + \frac{1}{a_{n+1}}\right)Q'_{n-1}} = \frac{P_{n-2} + \left(a_n + \frac{1}{a_{n+1}}\right)P_{n-1}}{Q_{n-2} + \left(a_n + \frac{1}{a_{n+1}}\right)Q_{n-1}} =$$

$$= \frac{P_{n-2} + a_n P_{n-1} + \frac{P_{n-1}}{a_{n+1}}}{Q_{n-2} + a_n Q_{n-1} + \frac{Q_{n-1}}{a_{n+1}}} = \frac{P_n + \frac{P_{n-1}}{a_{n+1}}}{Q_n + \frac{Q_{n-1}}{a_{n+1}}} = \frac{P_{n+1}}{Q_{n+1}}.$$

Заключение индукции: формула верна для любого числа n ($0 \le n \le s$): $A_n = P_n/Q_n$.

Теорема доказана.

Теорема 22. $P_n Q_{n-1} - P_{n-1} Q_n = (-1)^{n-1}$ для любого $n = 1, 2, \ldots, s$.

Доказательство (по принципу математической индукции).

База индукции:

$n = 1 \Rightarrow P_1 Q_0 - P_0 Q_1 = (a_0 a_1 + 1)1 - (a_0 a_1) = 1 = (-1)^{1-1}$.

Шаг индукции: предположим, что формула верна для некоторого n, и докажем, что формула верна для n+1.

Доказательство индукции:

$P_{n+1} Q_n - P_n Q_{n+1} = (P_{n-1} + P_n a_{n+1}) Q_n - P_n (Q_{n-1} + Q_n a_{n+1}) =$

$= P_{n-1} Q_n - P_n Q_{n-1} = (-1)(P_n Q_{n-1} - P_{n-1} Q_n) = (-1)(-1)^{n-1} = (-1)^n$.

Заключение индукции: формула верна для любого числа n ($0 \le n \le s$).

Теорема доказана.

Теорема 23. Дробь P_n / Q_n всегда несократима.

Доказательство. Пусть $d \mid P_n$, $d \mid Q_n$ (d – общий делитель P_n и Q_n). Тогда из предыдущей теоремы получаем $d \mid (-1)^{n-1}$, откуда следует, что $d = 1$.

Теорема доказана.

§ 14. Применение цепных дробей к решению линейных сравнений

Рассмотрим сравнение $a\,x \equiv 1 mod\, n$, где a и n взаимно простые.

$a/n = [a_0, a_1, \dots, a_s]$. Тогда $a/n = P_s/Q_s$ (причем, $a = P_s$, $n = Q_s$).

Имеем $P_s\,Q_{s-1} - P_{s-1}\,Q_s = (-1)^{s-1}$, т. е. $a\,Q_{s-1} - P_{s-1}\,n = (-1)^{s-1}$. Тогда в $\mathbb{Z}/n\mathbb{Z}$ выполняется $\overline{a}\,\overline{Q_{s-1}} = \overline{(-1)^{s-1}}$, откуда $\bar{x} = \bar{a}^{-1} = \overline{Q_{s-1}(-1)^{s-1}}$.

Пример 1. Решить сравнение с помощью цепных дробей: $1973x \equiv 1 \bmod 2579$.

Напомним, что решение сравнения $ax \equiv b \mod n$ находят по формуле $\bar{x} = \left(\overline{a}\right)^{-1}\bar{b}$.

Рассмотрим дробь 1973/2579.

$1973 = 0\cdot 2579 + 1973$ $\quad a_0 = 0$

$2579 = 1\cdot 1973 + 606$ $\quad a_1 = 1$

$1973 = 3\cdot 606 + 155$ $\quad a_2 = 3$

$606 = 3\cdot 155 + 141$ $\quad a_3 = 3$

$155 = 1\cdot 141 + 14$ $\quad a_4 = 1$

$141 = 10\cdot 14 + 1$ $\quad a_5 = 10$

$14 = 14\cdot 1 + 0$ $\quad a_6 = 14$

$1973/2579 = [0, 1, 3, 3, 1, 10, 14]$.

Вычисляем P_n и Q_n, используя рекуррентные формулы $P_n = a_n\,P_{n-1} + P_{n-2}$, $Q_n = a_n\,Q_{n-1} + Q_{n-2}$:

n	0	1	2	3	4	5	6
a_n	0	1	3	3	1	10	14
P_n	0	1	3	10	13	140	1973
Q_n	1	1	4	13	17	183	2579

По формуле перед примером в $\mathbb{Z}/2579\mathbb{Z}$ $\overline{1973}^{-1} = \overline{183}\,\overline{(-1)}^{5} = -\overline{183}$.

Ответ: $x = -183 + 2579z$, $z \in \mathbb{Z}$.

Пример 2. Решить сравнение $612x \equiv 1 \bmod 343$.

Рассмотрим дробь 612/343.

$612 = 1\cdot 343 + 269$ $\quad a_0 = 1$

$343 = 1\cdot 269 + 74$ $\quad a_1 = 1$

$269 = 3\cdot 74 + 47$ $a_2 = 3$
$74 = 1\cdot 47 + 27$ $a_3 = 1$
$47 = 1\cdot 27 + 20$ $a_4 = 1$
$27 = 1\cdot 20 + 7$ $a_5 = 1$
$20 = 2\cdot 7 + 6$ $a_6=2$
$7 = 1\cdot 6 + 1$ $a_7=1$
$6 = 6\cdot 1 + 0$ $a_8=6$
$612/343 = [1, 1, 3, 1, 1, 1, 2, 1, 6]$.
Вычисляем P_n и Q_n:

n	0	1	2	3	4	5	6	7	8
a_n	1	1	3	1	1	1	2	1	6
P_n	1	2	7	9	16	25	66	91	612
Q_n	1	1	4	5	9	74	37	51	343

Таким образом, в $\mathbb{Z}/343\mathbb{Z}$ $\overline{612}^{-1} = \overline{51}\overline{(-1)}^{7} = -\overline{51}$.
Ответ: $x = -51 + 343z,\ z\in\mathbb{Z}$.

Пример 3. Решить сравнение $1124x \equiv 1 \bmod 1029$.
Рассмотрим дробь 1124/1029.
$1124 = 1\cdot 1029 + 95$ $a_0 = 1$
$1029 = 10\cdot 95 + 79$ $a_1 = 10$
$95 = 1\cdot 79 + 16$ $a_2 = 1$
$79 = 4\cdot 16 + 15$ $a_3 = 4$
$16 = 1\cdot 15 + 1$ $a_4 = 1$
$15 = 15\cdot 1 + 0$ $a_5 = 15$
$1124/1029 = [1, 10, 1, 4, 1, 15]$.
Вычисляем P_n и Q_n:

N	0	1	2	3	4	5
a_n	1	10	1	4	1	15
P_n	1	11	12	59	71	1124
Q_n	1	10	11	54	65	1029

В $\mathbb{Z}/1029\mathbb{Z}$ $\overline{1124}^{-1} = \overline{65}\overline{(-1)}^{4} = \overline{65}$.
Ответ: $x = 65 + 1029z,\ z\in\mathbb{Z}$.

Задачи для самостоятельного решения

Решить сравнения: а) $613x \equiv 1 \bmod 1024$;
б) $523x \equiv 1 \bmod 729$, в) $707x \equiv 1 \bmod 1681$.
Ответ: а) $x = -147 + 1024z,\ z \in \mathbb{Z}$; б) $x = 46 + 729z,\ z \in \mathbb{Z}$;
в) $x = 447 + 1681z,\ z \in \mathbb{Z}$.

§ 15. Непрерывные дроби

Определение 15. Непрерывная дробь – бесконечная цепная дробь $a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}}$,

где $a_0 \in \mathbb{Z}$, $a_i \geq 1$, $a_i \in \mathbb{Z}$ при $i \geq 1$. Обозначение как и для цепных дробей: $[a_0, a_1, \ldots, a_n, \ldots] = \alpha$.

$A_n = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}$ – n-я подходящая дробь.

Значение цепной дроби $\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}}$

равно пределу A_n при $n \to \infty$: $\lim\limits_{n \to \infty} A_n = \alpha, \alpha \in \mathbb{R}$.

Определение 16. Непрерывная дробь называется периодической, если, начиная с некоторого номера, повторяется элемент a_n или некоторая группа элементов a_n, a_{n+1}, a_{n+k-1} (при этом k – период).

Пример 1. Найдем значение следующей периодической дроби: $\alpha = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ddots}}} = [1,\ 2,\ 2,\ \ldots]$.

Рассмотрим $\beta=2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+}}}\ddots=[2,\ 2,\ 2,...]$, $\beta=2+\frac{1}{\beta} \Rightarrow \Rightarrow \beta^2-2\beta-1=0 \Rightarrow$

$$\Rightarrow \beta=\frac{2+\sqrt{8}}{2}=1+\sqrt{2}.$$

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

Пример 2. Найти значение α = [0, 1, 2, 3, 3, 3, …].

Рассмотрим β = [3, 3, …, 3, …]= $3+\cfrac{1}{3+\cfrac{1}{3+\cfrac{1}{3+}}}\ddots$.

$$\beta=3+\frac{1}{\beta} \Rightarrow \beta^2-3\beta-1=0 \Rightarrow \beta=\frac{3+\sqrt{13}}{2} \Rightarrow \beta=\frac{3+\sqrt{13}}{2}\ (\beta>0).$$

По условию $\alpha=\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{\beta}}}=[0,\ 1,\ 2,\ \beta]$.

Чтобы найти α, применяем табличную форму, которую мы использовали в предыдущем параграфе:

n	0	1	2	3
a_n	0	1	2	β
P_n	0	1	2	2β+1
Q_n	1	1	3	3β+1

$$\alpha=\frac{1+2\beta}{1+3\beta}=\frac{1+3+\sqrt{13}}{1+3\frac{3+\sqrt{13}}{2}}=\frac{8+2\sqrt{13}}{11+3\sqrt{13}}.$$

Вычисление периодической дроби с периодом больше 1.

Пример 3. Пусть $\alpha = [1, 2, \underline{3, 1, 1}, \underline{3, 1, 1}\ldots]$,
$\beta = [3, 1, 1, 3, 1, 1\ldots]$.

Тогда $\beta = [3, 1, 1, \beta]$, $\alpha = [1, 2, \beta]$ – обобщенные цепные конечные дроби;

n	0	1	2
a_n	1	2	β
P_n	1	3	$3\beta+1$
Q_n	1	2	$2\beta+1$

$$\Rightarrow \quad \alpha=\frac{1+3\beta}{1+2\beta}.$$

n	0	1	2	3
a_n	3	1	1	β
P_n	3	4	7	$7\beta+4$
Q_n	1	1	2	$2\beta+1$

$$\Rightarrow \quad \beta=\frac{4+7\beta}{1+2\beta};$$

$$2\beta^2+\beta-4-7\beta=0 \Rightarrow \beta^2-3\beta-2=0 \Rightarrow \beta=\frac{3+\sqrt{17}}{2}.$$

$$\alpha=\frac{1+\dfrac{9+3\sqrt{17}}{2}}{1+\dfrac{6+2\sqrt{17}}{2}}=\frac{11+3\sqrt{17}}{8+2\sqrt{17}}=\frac{(11+3\sqrt{17})(2\sqrt{17}-8)}{(8+2\sqrt{17})(2\sqrt{17}-8)}=\frac{7-\sqrt{17}}{2}.$$

Обзор основных результатов по непрерывным дробям

Теорема 23. Любая бесконечная непрерывная дробь сходится.

Теорема 24. Любое вещественное число α однозначно представляется в виде непрерывной дроби: рациональные – конечными, иррациональные – бесконечными дробями.

Определение 17. Назовем квадратичной иррациональностью число вида $\dfrac{a+b\sqrt{c}}{d}$, где $\sqrt{c}\notin\mathbb{Q}$; $a, b, c, d\in\mathbb{Z}$, $d\neq 0$.

Теорема 25. Любая периодическая непрерывная дробь сходится к квадратичной иррациональности.

Теорема Лагранжа. Любую квадратичную иррациональность можно представить в виде периодической непрерывной дроби.

Пример. Представить $\sqrt{6}$ в виде периодической дроби.

$\alpha=\sqrt{6}=2, \ldots$

$$\alpha = 2 + \frac{1}{y_1},\ y_1 > 1;\ \frac{1}{y_1} = \sqrt{6} - 2 \Rightarrow$$

$$\Rightarrow y_1 = \frac{1}{\sqrt{6}-2} = \frac{\sqrt{6}+2}{2} = \frac{4,\ ...}{2} = 2,\ ...$$

$$y_1 = 2 + \frac{1}{y_2};\ \frac{1}{y_2} = \frac{\sqrt{6}+2}{2} - 2 = \frac{\sqrt{6}-2}{2} \Rightarrow$$

$$\Rightarrow\ y_2 = \frac{2}{\sqrt{6}-2} = \sqrt{6}+2 = 4 + \frac{1}{y_3};$$

$\frac{1}{y_3} = \sqrt{6} - 2 \Rightarrow y_3 = \frac{1}{\sqrt{6}-2} = \frac{\sqrt{6}+2}{2} = y_1$. Следовательно, α = [2, 2, 4, 2, 4, …] – периодическая непрерывная дробь.

Пример. Представить $\sqrt{7}$ в виде периодической дроби.

$$\alpha = \sqrt{7} = 2,\ ...$$

$$\alpha = 2 + \frac{1}{y_1},\ y_1 > 1;$$

$$\frac{1}{y_1} = \sqrt{7} - 2 \Rightarrow y_1 = \frac{1}{\sqrt{7}-2} = \frac{\sqrt{7}+2}{3} = \frac{4,\ ...}{3} = 1,\ ...$$

$$y_1 = 1 + \frac{1}{y_2};\ \frac{1}{y_2} = \frac{\sqrt{7}-1}{3} \Rightarrow$$

$$\Rightarrow\ y_2 = \frac{3}{\sqrt{7}-1} = \frac{3\sqrt{7}+3}{6} = \frac{\sqrt{7}+1}{2} = 1,\ ... = 1 + \frac{1}{y_3};$$

$$\frac{1}{y_3} = \frac{\sqrt{7}+1-2}{2} = \frac{\sqrt{7}-1}{2} \Rightarrow$$

$$\Rightarrow y_3 = \frac{2}{\sqrt{7}-1} = \frac{2(\sqrt{7}+1)}{6} = \frac{\sqrt{7}+1}{3} = 1,\ ... = 1 + \frac{1}{y^4};$$

$$\frac{1}{y_4} = \frac{\sqrt{7}+1-3}{3} = \frac{\sqrt{7}-2}{3} \Rightarrow$$

$$\Rightarrow y_4 = \frac{3}{\sqrt{7}-2} = \frac{3(\sqrt{7}+2)}{3} = \sqrt{7}+2 = 4,\ ... = 4 + \frac{1}{y_5};$$

$\frac{1}{y_5} = \sqrt{7} - 2 \Rightarrow y_5 = \frac{1}{\sqrt{7}-2} = \frac{\sqrt{7}+2}{3} = 1,\ ...$ Так как $y_5 = y_1$, то α = [2, 1, 1, 1, 4, 1, 1, 1, 4, …] – периодическая непрерывная дробь.

§ 16. Разложение по степеням двучлена по схеме Горнера

Пусть $f(x) = a_n x^n + \ldots + a_1 x + a_0$. Найдем $f(\gamma)$, где γ – некоторое число. Ясно, что

$a_n x^n + \ldots + a_1 x + a_0 = (x - \gamma)(b_{n-1} x^{n-1} + \ldots + b_1 x + b_0) + f(\gamma)$ для некоторых b_i. Приравниваем коэффициенты при одинаковых степенях x в левой и правой части:

$$\begin{cases} a_n = b_{n-1}; \\ a_{n-1} = b_{n-2} - \gamma b_{n-1}; \\ \ldots \\ a_2 = b_1 - \gamma b_2; \\ a_1 = b_0 - \gamma b_1; \\ a_0 = f(\gamma) - \gamma b_0; \end{cases} \Rightarrow \begin{cases} b_{n-1} = a_n; \\ b_{n-2} = \gamma b_{n-1} + a_{n-1}; \\ \ldots \\ b_1 = \gamma b_2 + a_2; \\ b_0 = \gamma b_1 + a_1; \\ f(\gamma) = \gamma b_0 + a_0. \end{cases}$$

Вычисление коэффициентов b_i и $f(\gamma)$ можно организовать в следующем виде:

–	a_n	a_{n-1}	a_{n-2}	…	a_2	a_1	a_0
γ	b_{n-1}	b_{n-2}	b_{n-3}	…	b_1	b_0	$f(\gamma)$

Пример. $f(x) = 13x^4 + 9x^3 + 7x^2 + 5x + 2$, $\gamma = 3$.

–	13	9	7	5	2
3	13	48	151	458	1376

Получили $f(x) = (x - 3)(13x^3 + 48x^2 + 151x + 458) + 1376$, откуда $f(3) = 1376$.

Теперь займемся разложением $f(x)$ по степеням $(x - \gamma)$.

Пусть снова $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ – многочлен степени n. Обозначим $f(x) = f_n(x)$.

$f(x) = (x - \gamma)(b_{n-1} x^{n-1} + \ldots + b_1 x + b_0) + f(\gamma)$.

Применяем схему Горнера для $f_{n-1}(x) = b_{n-1} x^{n-1} + \ldots + b_1 x + b_0$ с тем же γ:

$f(x) = (x - \gamma)((x - \gamma)(c_{n-2} x^{n-2} + \ldots + c_1 x + c_0) + f_{n-1}(\gamma)) + f(\gamma) =$

$= (x - \gamma)^2 f_{n-2}(x) + f_{n-1}(\gamma)(x - \gamma) + f(\gamma)$.

Продолжая указанный процесс, в итоге получим разложение $f(x)$ по степеням $(x - \gamma)$.

Пример 1. Разложить $f(x) = 3x^4 + 2x^3 - 9x^2 + 7x - 5$ по степеням $(x - 2)$, используя схему Горнера:

–	3	2	−9	7	−5
2	3	8	7	21	37
2	3	14	35	91	
2	3	20	75		
2	3	26			
2	3				

Получили $f(x) = 3(x - 2)^4 + 26(x - 2)^3 + 75(x - 2)^2 + 91(x - 2) + 37$.

Пример 2. Разложить $f(x) = 3x^4 + 2x^3 - 9x^2 + 7x - 5$ по степеням $(x + 3)$, используя схему Горнера:

–	3	2	−9	7	−5
−3	3	−7	12	−29	82
−3	3	−16	60	−209	
−3	3	−25	135		
−3	3	−34			
−3	3				

Получили $f(x) = 3(x + 3)^4 - 34(x + 3)^3 + 135(x + 3)^2 - 209(x + 3) + 82$.

§ 17. Применение цепных дробей к приближенному решению уравнений

Рассмотрим данный метод на примере. Пусть требуется решить уравнение $x^3 + 2x - 4 = 0$.

Обозначим $f(x) = x^3 + 2x - 4$. Тогда $f'(x) = 3x^2 + 2 > 0 \Rightarrow f(x)$ имеет единственный корень. Так как $f(1) = -1$, а $f(2) = 8$, то этот корень α лежит на интервале (1, 2). Стало быть, $\alpha = 1 + \frac{1}{y_1}, y_1 > 1$..

Раскладываем $f(x)$ по степеням $(x-1)$ по схеме Горнера:

–	1	0	2	−4
1	1	1	3	−1
1	1	2	5	
1	1	3		
1	1			

Получили $f(x) = (x-1)^3 + 3(x-1)^2 + 5(x-1) - 1$.

$$f(\alpha) = \frac{1}{y_1^3} + \frac{3}{y_1^2} + \frac{5}{y_3} - 1 = \frac{-y_1^3 + 5y_1^2 + 3y_1 + 1}{y_1^3} = 0.$$

Поэтому y_1 – единственный корень многочлена $g(y) = y^3 - 5y^2 - 3y - 1$ на $(1, +\infty)$, так как иначе $f(x)$ имел бы два корня на $(1, 2)$. Из того, что $g(5) < 0$, $g(6) > 0$, следует $5 < y_1 < 6$, т. е. $y_1 = 5 + \frac{1}{y_2}, y_2 > 1$.

Раскладываем $g(y)$ по степеням $(y-5)$.

–	1	−5	−3	−1
5	1	0	−3	−16
5	1	5	22	
5	1	10		
5	1			

Таким образом, $g(y) = (y-5)^3 + 10(y-5)^2 + 22(y-5) - 16$.

$$g(y_1) = \frac{1}{y_2^3} + \frac{10}{y_2^2} + \frac{22}{y_2} - 16 = \frac{-16y_2^3 + 22y_2^2 + 10y_2 + 1}{y_2^3} = 0 \Rightarrow$$

y_2 – единственный корень многочлена $h(y) = 16y^3 - 22y^2 - 10y - 1$ на $(1, +\infty)$. Из того $h(1)<0$, $h(2)>0$, следует, что $y_2 \in (1, 2)$, т. е. $y_2 = 1 + \frac{1}{y_3}, y_3 > 1$.

Раскладываем $h(y)$ по степеням $(y-1)$:

–	16	−22	−10	−1
1	16	−6	−16	−17
1	16	10	−6	
1	16	26		
1	16			

$h(y) = 16(y-1)^3 + 26(y-1)^2 - 6(y-5) - 17.$

$$h(y_2)=\frac{16}{y_3^3}+\frac{26}{y_3^2}-\frac{6}{y_3}-17=\frac{-17y_3^3-6y_3^2+26y_3+16}{y_3^3}=0 \Rightarrow$$

y_3 – единственный корень многочлена $\varphi(y)=17y_3^3+6y_3^2-26y_3-16$ на $(1, +\infty)$. Так как $\varphi(1) < 0$, $\varphi(2) > 0$, то $1 < y_3 < 2$.

Здесь мы остановим процесс вычисления, хотя его можно продолжать бесконечно.

Имеем по построению

$$\alpha=[1,5,1,y_3]=1+\cfrac{1}{5+\cfrac{1}{1+\cfrac{1}{y_3}}},$$

где $y_3 \in (1,2)$.

Посчитаем α с помощью известной нам табличной формы:

n	0	1	2	3
a_n	1	5	1	y_3
P_n	1	6	7	$7y_3 + 6$
Q_n	1	5	6	$6y_3 + 5$

Таким образом, $\alpha=\dfrac{7y_3+6}{6y_3+5}$.

При $y_3=1$ $\alpha=\dfrac{13}{11}$, при $y_3=2$ $\alpha=\dfrac{20}{17}$.

Следовательно, $\dfrac{20}{17}<\alpha<\dfrac{13}{11}$, $\dfrac{13}{11}-\dfrac{20}{17}=\dfrac{1}{187}$.

Ответ: $\alpha\approx\dfrac{20}{17}$ с погрешностью $<\dfrac{1}{187}$.

Задачи для самостоятельного решения

1) Разложить многочлены $f(x)$ и $g(x)$ по указанным степеням: а) $f(x)=4x^3+7x^2+5x+3$ по степеням $(x+4)$; б) $g(x)=x^4-5x^2-x-2$ по степеням $(x-5)$.

2) Найти все вещественные корни многочленов $f(x)$, $g(x)$ с точностью до 0,001, пользуясь цепными дробями: $f(x)=x^3-2x^2+2x-3$, $g(x)=x^3+3x^2-3$.

ГЛАВА IV. СРАВНЕНИЯ ПО МОДУЛЮ p^k И p-АДИЧЕСКИЕ ЧИСЛА

§ 18. Решение сравнений по модулю p^k

Рассмотрим сравнение $a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \equiv 0 \bmod p^k$, $k \geq 1$, p – простое число. Обозначим $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$.

Лемма 3. 1. $f(a) \equiv 0 \bmod p^k \Leftrightarrow f(\bar{a}) = \bar{0}$ в $\mathbb{Z}/\mathrm{p^k}\mathbb{Z}$;

2. если a удовлетворяет сравнению $f(a) \equiv 0 \bmod p^k$, то все числа из класса $\bar{a} = a + p^k\mathbb{Z}$ также удовлетворяют этому сравнению ($a \in \mathbb{Z}$).

Доказательство.

1. $f(a) \equiv 0 \bmod p^k \Leftrightarrow \overline{a_n a^n + a_{n-1}a^{n-1} + ... + a_1 a + a_0} = \bar{0} \Leftrightarrow$

$\Leftrightarrow \bar{a}_n \bar{a}^n + \bar{a}_{n-1}\bar{a}^{n-1} + ... + \bar{a}_1\bar{a} + \bar{a}_0 = \bar{0}$, где $\bar{a}_i \in \mathbb{Z}/\,p^k\mathbb{Z}, \Leftrightarrow f(\bar{a}) = \bar{0}$.

2. $f(a) \equiv 0 \bmod p^k \Rightarrow \bar{a}_n \bar{a}^n + \bar{a}_{n-1}\bar{a}^{n-1} + ... + \bar{a}_1\bar{a} + \bar{a}_0 = \bar{0}$, следовательно, все числа из $\bar{a} = a + p^k\mathbb{Z}$ удовлетворяют сравнению $f(x) \equiv 0 \bmod p^k$.

Лемма доказана.

Теорема (аналог леммы Гензеля в алгебраической теории чисел). Пусть $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \in \mathbb{Z}[x]$, $f(a) \equiv 0 \bmod p^k$, $k \in \mathbb{N}$, $f'(a) \not\equiv 0 \bmod p^k$. Тогда среди чисел класса вычетов $a + p^k\mathbb{Z}$ сравнению $f(x) \equiv 0 \bmod p^{k+1}$ удовлетворяют все числа некоторого единственного класса вычетов по модулю p^{k+1}.

Доказательство.

$a + p^k\mathbb{Z}$ разбивается на p классов вычетов по модулю p^{k+1}:

$$(a + 0\cdot p^k + p^{k+1}\mathbb{Z}) \cup (a + 1\cdot p^k + p^{k+1}\mathbb{Z}) \cup (a + 2p^k + p^{k+1}\mathbb{Z}) \cup$$
$$\cup ... \cup (a + (p-1)p^k + p^{k+1}\mathbb{Z}).$$

Все указанные классы различны, так как их представители не сравнимы с нулем по модулю p^{k+1}. Требуется доказать, что из этих p классов только один удовлетворяет сравнению $f(x) \equiv 0 \bmod p^k$.

Рассмотрим число $a + p^k t$ и используем формулу Тейлора:

$$f(a + p^k t) = f(a) + \frac{f'(a)}{1!}(p^k t) + \frac{f''(a)}{2!}(p^k t)^2 + ... + \frac{f^{(n)}(a)}{n!}(p^k t)^n.$$

Все члены справа, начиная с третьего, делятся на p^{k+1}. Тогда $f(a+p^k t)\equiv 0 \bmod p^{k+1} \Leftrightarrow f(a)+f'(a)p^k t\equiv 0 \bmod p^{k+1}$. Так как $f(a)\equiv 0 \bmod p^k$, то $\frac{f(a)}{p^k}$ – целое число, следовательно, имеем сравнение $f'(a)t+\frac{f(a)}{p^k}\equiv 0 \bmod p$. Так как $f'(a)\not\equiv 0 \bmod p$, то t определяется однозначно по модулю p.

Теорема доказана.

Следствие. Пусть $f(a)\equiv 0 \bmod p$, $f'(a)\not\equiv 0 \bmod p$. Тогда существует единственная бесконечная последовательность классов вычетов по модулю $p, p^2, \ldots, p^k, \ldots$: $\bar{x}_1=\bar{a}$ в $\mathbb{Z}/p\mathbb{Z}$, $\bar{x}_2$ в $\mathbb{Z}/p^2\mathbb{Z}, \ldots$ $\bar{x}_k$ в $\mathbb{Z}/p^k\mathbb{Z}, \ldots$, для которой $x_{k+1}\equiv x_k \bmod p^k$ для любого $k\geq 1$, и x_k удовлетворяет сравнению $f(x)\equiv 0 \bmod p^k$.

Доказательство.

Пусть $\bar{a}=\bar{x}_1$. Из теоремы следует, что в $\mathbb{Z}/p^2\mathbb{Z}$ существует $\bar{x}_2$, удовлетворяющий сравнению $f(x)\equiv 0 \bmod p^2$, $x_2\equiv x_1 \bmod p$. Для $\bar{x}_2$ находим $\bar{x}_3$ в $\mathbb{Z}/p^3\mathbb{Z}$, удовлетворяющий сравнению $f(x)\equiv 0 \bmod p^3$, $x_3\equiv x_2 \bmod p^2$ и т. д.

Следствие доказано.

Пример 1. Решить сравнение $x^2+2x+4\equiv 0 \bmod 7^4$.

Рассмотрим сравнение $x^2+2x+4\equiv 0 \bmod 7$ в $\mathbb{Z}/7\mathbb{Z}$. Подбором находим числа $x_1 = 1$, $x_2 = 4$, удовлетворяющие этому сравнению.

$$f'(x)=2x+2,\ f'(x_1)=4\neq 0 \text{ в } \mathbb{Z}/7\mathbb{Z},\ f'(x_2)=3\neq 0 \text{ в } \mathbb{Z}/7\mathbb{Z}.$$

1) Поднимаем x_1 на высоту 2, т. е. находим решение x_2' сравнения $f(x)\equiv 0 \bmod 7^2$ такое, что $x_2'\equiv x_1 \bmod 7$.

$$f'(1)t+\frac{f(1)}{7}\equiv 0 \bmod 7;\ 4t+1\equiv 0 \bmod 7;\ t=-2 \text{ по модулю } 7.$$

Тогда $1+7(-2)=-13=a+p^1 t$ – решение сравнения $f(x)\equiv 0 \bmod 7^2$.

2) Поднимаем (–13) на высоту 3, т. е. находим решение x_3' сравнения $f(x)\equiv 0 \bmod 7^3$ такое, при котором $x_3'\equiv x_2' \bmod 49$.

$f(-13)=147$ (должно делиться на 7^2).

$$f'(1)t+\frac{f(-13)}{49}\equiv 0 \bmod 7;\ 4t+3\equiv 0 \bmod 7;\ t=1 \text{ по модулю } 7.$$

Тогда $a+p^2t=-13+49\cdot 1=36$ – решение сравнения $f(x)\equiv 0 \bmod 7^3$.

$f(36)=1296+72+4=1372=343\cdot 4$.

3) Поднимаем 36 на высоту 4:

$$f'(1)t+\frac{f(36)}{343}\equiv 0 \bmod 7;\ 4t+4\equiv 0 \bmod 7;\ t=-1 \text{ по модулю } 7.$$

Тогда $a+p^3t=36+343\cdot(-1)=-307$ – решение сравнения $f(x)\equiv 0 \bmod 7^4$.

$x_1=-307+2401z,\ z\in\mathbb{Z}$.

Аналогично для $x_2=4$.

4) $$f'(4)t+\frac{f(4)}{7}\equiv 0 \bmod 7;\ 3t+4\equiv 0 \bmod 7;$$

$t=1$ по модулю 7.

$a+pt=4+7\cdot 1=11$ – решение сравнения $f(x)\equiv 0 \bmod 7^2$.

$f(11)=121+22+4=147$.

5) $$f'(4)t+\frac{f(11)}{49}\equiv 0 \bmod 7;\ 3t+3\equiv 0 \bmod 7;$$

$t=-1$ по модулю 7.

$a+p^2t=11+49(-1)=-38$ – решение сравнения $f(x)\equiv 0 \bmod 7^3$.

$f(-38)=1444-76+4=1372=343\cdot 4$.

6) $$f'(4)t+\frac{f(-38)}{343}\equiv 0 \bmod 7;\ 3t+4\equiv 0 \bmod 7;$$

$t=1$ по модулю 7.

$a+p^3t=-38+343\cdot 1=305$ – решение сравнения $f(x)\equiv 0 \bmod 7^4$.

$x_2=305+2401z,\ z\in\mathbb{Z}$.

Ответ: $x_1=-307+2401z$, $x_2=305+2401z,\ z\in\mathbb{Z}$.

Пример 2. Извлечь корни 4-й степени из (–1) в $\mathbb{Z}/289\mathbb{Z}$.

Решение. Заметим сначала, что $289=17^2$, и обозначим $f(x)=x^4+1$. Тогда $f'(x)=4x^3$.

Подбором находим два решения сравнения $x^4+1\equiv 0 \bmod 17$: $x_{1,2}=\pm 2$. Чтобы найти остальные решения, поделим x^4+1 уголком на $(x-x_1)(x-x_2)=x^2-4$ в $\mathbb{Z}/17\mathbb{Z}$. Получим $x^4+1=(x^2-4)(x^2+4)$. Также подбором находим два решения сравнения $x^2+4\equiv 0 \bmod 17$: $x_{1,2}=\pm 8$.

Поднимаем решение $x_1 = 2$ исходного сравнения на высоту 2 т. е. найдем решение x_2' сравнения $x^4+1\equiv 0 \bmod 289$ такое что $x_2' \equiv x_1 \bmod 17$. Для этого решим сравнение $f'(2)t+\dfrac{f(2)}{17}\equiv 0 \bmod 17$, т. е. $-2t+1\equiv 0 \bmod 17$. Находим подбором $t = 9$. Поэтому $2+17\cdot 9=155$ – решение сравнения $x^4+1\equiv 0 \bmod 289$. Тогда ясно, что (-155) – также решение этого сравнения.

Поднимем теперь решение $x_3 = 8$ исходного сравнения на высоту 2. Для этого решаем сравнение $f'(8)t+\dfrac{f(8)}{17}\equiv 0 \bmod 17$, т. е. $8t+241\equiv 0 \bmod 17$ или $8t+3\equiv 0 \bmod 17$. Находим подбором $t = 6$. Следовательно, $8+17\cdot 6=110$ – решение сравнения $x^4+1\equiv 0 \bmod 289$. Тогда и (-110) – тоже решение этого сравнения.

Ответ: $\pm\overline{155}, \pm\overline{110}$ – корни 4-й степени из (-1) в $\mathbb{Z}/289\mathbb{Z}$.

Задачи для самостоятельного решения

Решить сравнения:

1) $3x^2+4x+3\equiv 0 \bmod 7^4$; 2) $2x^2+3x+1\equiv 0 \bmod 5^4$;

3) $x^2+3x+3\equiv 0 \bmod 7^4$.

Ответы: 1) $x_1 = 2068+7^4 z$, $x_2 = 1132+7^4 z$, $z\in\mathbb{Z}$;

2) $x_1 = -1+5^4 z$, $x_2 = 312+5^4 z$, $z\in\mathbb{Z}$;

3) $x_1 = 1352+7^4 z$, $x_2 = 1046+7^4 z$, $z\in\mathbb{Z}$.

§ 19. p-адические числа

Определение 18. Целым p-адическим числом называется бесконечная последовательность $\ldots \bar{\alpha}_n, \bar{\alpha}_{n-1}, \ldots, \bar{\alpha}_1$, где $\forall n\ \bar{\alpha}_n \in \mathbb{Z}/p^n\mathbb{Z}$, причем $\forall n \geq 2\ \alpha_n \equiv \alpha_{n-1} \bmod p^{n-1}$, т. е. $\alpha_n + p^{n-1}\mathbb{Z} = \alpha_{n-1} + p^{n-1}\mathbb{Z}$.

Примеры.

1) $\ldots, 65+7^3\mathbb{Z}, 16+7^2\mathbb{Z}, 2+7\mathbb{Z}$.

2) $\ldots, 43+2^5\mathbb{Z}, 11+2^4\mathbb{Z}, 11+2^3\mathbb{Z}, 3+2^2\mathbb{Z}, 1+2\mathbb{Z}$.

Множество всех целых p-адических чисел обозначается как Z_p.

Если все α_n – канонические представители соответствующих классов вычетов, т. е. $0\leq\alpha_n < p^n\ \forall n\in\mathbb{N}$, то из определения 18 следует,

что $0 \le \alpha_1 < p, \alpha_2 = \alpha_1 + \gamma_2 p$, где $0 \le \gamma_2 < p$; $\alpha_3 = \alpha_2 + \gamma_3 p^2$, где $0 \le \gamma_3 < p^2$ и т. д. Следовательно, p-адическое число $\ldots \bar{\alpha}_n, \bar{\alpha}_{n-1}, \ldots, \bar{\alpha}_1$ можно записать в позиционной записи $\ldots \gamma_n, \gamma_{n-1}, \ldots, \gamma_1$, где $\forall n \in \mathbb{N}\ 0 \le \gamma_n < p^n$, или более наглядно в виде $\ldots + \gamma_n p^{n-1} + \ldots + \gamma_2 p + \gamma_1$, где $\gamma_1 = \alpha_1$.

Определение 19.

Если $\alpha = \ldots \bar{\alpha}_n, \bar{\alpha}_{n-1}, \ldots \bar{\alpha}_1$ и $\beta = \ldots \bar{\beta}_n, \bar{\beta}_{n-1}, \ldots \bar{\beta}_1$ – два p-адических числа, то $\alpha + \beta = \ldots \bar{\alpha}_n + \bar{\beta}_n, \bar{\alpha}_{n-1} + \bar{\beta}_{n-1}, \ldots, \bar{\alpha}_1 + \bar{\beta}_1$; $\alpha \cdot \beta = \ldots \overline{\alpha_n \beta_n}, \overline{\alpha_{n-1}\beta_{n-1}}, \ldots, \overline{\alpha_1 \beta_1}$.

Теорема 26.

1) $\mathbb{Z}_p$ является коммутативным ассоциативным кольцом относительно вышеопределенных операций сложения и умножения с кольцевой единицей в позиционной записи …0…01 и кольцевым нулем …00…0.

2) Мультипликативная группа $\mathbb{Z}_p^*$ данного кольца состоит из всех p-адических чисел $\ldots \bar{\alpha}_n \bar{\alpha}_{n-1} \ldots \bar{\alpha}_1$, где $\alpha_1 \not\equiv 1 \bmod p$.

Доказательство следует из покомпонентности сложения и умножения p-адических чисел.

Если $\ldots \gamma_n, \gamma_{n-1}, \ldots, \gamma_1$ позиционная запись p-адического числа α, то $\alpha = \ldots \overline{\gamma_n p^{n-1} + \gamma_{n-1} p^{n-2} + \ldots + \gamma_1}, \overline{\gamma_{n-1} p^{n-2} + \ldots + \gamma_1}, \ldots, \overline{\gamma_1}$, откуда следует, что в позиционной записи p-адические числа складываются и перемножаются столбиком (по обычным школьным правилам), однако действия над числами в отдельных позициях производятся по модулю p.

Пример. В кольце $\mathbb{Z}_7$ $\begin{array}{r} \ldots 54321 \\ + \ \ldots 65142 \\ \hline \ldots 152463 \end{array}$.

Здесь при сложении чисел в четвертой позиции получилось число $9 = 1 \cdot 7 + 2$, поэтому в этой позиции в сумме пишем 2, а единицу, стоящую перед 7, переносим налево, т. е. при сложении чисел в пятой позиции имеем $5 + 6 = 11 = 1 \cdot 7 + 4$, но в сумме вместо 4 пишем в пятой позиции 5, учитывая единицу переноса из 4-й позиции.

Далее ясно, что отображение $\varphi: \mathbb{Z} \to \mathbb{Z}_p$ такое, при котором $\forall z \in \mathbb{Z}\ \varphi(z) = \ldots, \overline{z}, \ldots, \overline{z}$, где справа в каждой позиции стоит $\overline{z}$, является изоморфным вложением $\mathbb{Z}$ в $\mathbb{Z}_p$, так что можно считать $\mathbb{Z} \subset \mathbb{Z}_p$.

Однако заметим, что если позиционная запись натурального числа имеет конечный вид $\gamma_n\gamma_{n-1}...,\gamma_1$, то позиционная запись отрицательного целого числа имеет бесконечный вид, например, -1 в $\mathbb{Z}_7$ равен …6…666 (6 в периоде).

На языке p-адических чисел рассмотренная нами теория в предыдущем параграфе говорит о том, что если a – решение уравнения $f(x) = 0$ в $\mathbb{Z}/p\mathbb{Z}$, где $f(x)$ – многочлен с целыми коэффициентами, причем $f'(a)\not\equiv 0 \bmod p$, то решение $\bar{a}$ поднимается до решения $...\bar{a}_n,...,\bar{a}_2,\bar{a}_1$, где $a_1 = a_2$, уравнения $f(x)=0$ в $\mathbb{Z}_p$.

Закончим этот параграф формулировкой знаменитой теоремы Хассе−Минковского.

Определение 20. Поле дробей кольца $\mathbb{Z}_p$ называется полем p-адических чисел. Оно обозначается $\mathbb{Q}_p$. Из теоремы 26 следует, что каждое ненулевое число из $\mathbb{Q}_p$ имеет вид xp^m, где $m\in\mathbb{Z}, x\in\mathbb{Z}_p^*$.

Теорема Хассе−Минковского. Невырожденная квадратичная форма с рациональными коэффициентами представляет 0 в $\mathbb{Q}$ (т. е. обращается в ноль при некоторых значениях переменных, причем не все эти значения равны 0) тогда и только тогда, когда эта форма представляет 0 в $\mathbb{Q}_p$ для любого простого p.

Очень нетривиально здесь доказательство достаточности, которое можно найти, например в книге [4].

Пример 1. Решить сравнение $221x \equiv 289 \bmod 7^3$.

Представляем числа 221 и 289 как 7-адические числа в позиционной записи:

$289 = 5\cdot 49 + 6\cdot 7 + 2\cdot 7^0 = \ldots 00562$, $221 = 4\cdot 49 + 3\cdot 7 + 4\cdot 7^0 = \ldots 00434$.

В $\mathbb{Z}_7$ равенство $x=\dfrac{562}{434}$ эквивалентно равенству $562 = 434\cdot x$. Чтобы найти нужное число первых цифр в позиционной записи x для решения данного сравнения, воспользуемся правилом умножения p-адических чисел столбиком:

$$
\begin{array}{r}
434 \\
\underline{...354} \\
2402 \\
3136 \\
1635 \\
\hline
00562
\end{array}
$$

Здесь x=...354 находится по первому множителю 434 и по результату 562 умножения 434 на x. Для решения сравнения по модулю 7^3 достаточно найти первые три цифры в позиционной записи x в $\mathbb{Z}_7$. И, наконец, переводим 7-адическое число 354 в десятичную запись: $354 = 3\cdot 49 + 5\cdot 7 + 4 = 147 + 39 = 186$.

Ответ: x=186+343$\mathbb{Z}$.

Пример 2. Решить сравнения $991x \equiv 878 \bmod 7^4$, $991x \equiv 878 \bmod 7^5$, $991x \equiv 878 \bmod 7^6$:

$878 = 2\cdot 343 + 3\cdot 49 + 6\cdot 7 + 3\cdot 7^0 = 2363_7$,

$991 = 2\cdot 343 + 6\cdot 49 + 1\cdot 7 + 4\cdot 7^0 = 2614_7$.

$x = \dfrac{2363}{2614}$; $2363 = 2614\cdot x$.

$$\begin{array}{r} 2614 \\ 40016 \\ \hline 23223 \\ 2614 \\ 000 \\ 00 \\ 14362 \\ 0 \\ \hline 02363 \end{array}$$

$016_7 = 7 + 6 = 13_{10}$, тогда $x = 13 + 7^4\mathbb{Z}$.

$40016 = 4\cdot 2401 + 7 + 6 = 9617$,

$x = 9617 + 7^5\mathbb{Z}$, $x = 9617 + 7^6\mathbb{Z}$.

Ответ: $x = 13 + 7^4\mathbb{Z}$, $x = 9617 + 7^5\mathbb{Z}$, $x = 9617 + 7^6\mathbb{Z}$.

Задачи для самостоятельного решения

Решить сравнения:

1) $57x \equiv 119 \bmod 2^7$; 2) $1278x \equiv 2279 \bmod 5^4$;

3) $1278x \equiv 2279 \bmod 5^6$; 4) $1278x \equiv 2279 \bmod 7^4$;

5) $1278x \equiv 2279 \bmod 7^6$.

Ответы: 1) $x = 47 + 2^7 z$, $z \in \mathbb{Z}$; 2) $x = 193 + 5^4 z$, $z \in \mathbb{Z}$;

3) $x = 2086 + 5^6 z$, $z \in \mathbb{Z}$; 4) $x = 680 + 7^4 z$, $z \in \mathbb{Z}$;

5) $x = 48700 + 7^6 z$, $z \in \mathbb{Z}$.

СПИСОК ЛИТЕРАТУРЫ

1. Бухштаб А. А. Теория чисел / А. А. Бухштаб. – М.: Просвещение, 1966.
2. Виноградов И. М. Основы теории чисел / И. М. Виноградов. – М.: Наука, 1972.
3. Дэвенпорт Г. Высшая арифметика / Г. Дэвенпорт. – М.: Наука, 1965.
4. Серр Ж.-П. Курс арифметики / Ж.-П. Серр. – М. : Мир, 1972.
5. Кострикин А. И. Введение в алгебру / А. И. Кострикин. – М.: Наука, 1977.
6. Боревич З. И. Теория чисел / З. И. Боревич, И. Р. Шафаревич. – М.: Наука, 1972.
7. Кудреватов Г. А. Сборник задач по теории чисел / Г. А. Кудреватов. – М.: Просвещение, 1970.
8. Александров В. А. Задачник-практикум по теории чисел / В. А. Александров, С. М. Горшенин. – М.: Просвещение, 1972.

Учебное пособие

Веретенников Борис Михайлович
Михалева Марина Михайловна

Алгебра и теория чисел
Часть I

Редактор *О. С. Смирнова*
Компьютерный набор *М. М. Михалевой*
Компьютерная верстка *Т. С. Криницыной*

Подписано в печать 30.05.2014. Формат 60×90 1/16.
Бумага писчая. Плоская печать. Усл. печ. л. 3,25.
Уч.-изд. л. 3,1. Тираж 100 экз. Заказ № 1164.

Издательство Уральского университета
Редакционно-издательский отдел ИПЦ УрФУ
620049, Екатеринбург, ул. С. Ковалевской, 5
Тел.: 8 (343) 375-48-25, 375-46-85, 374-19-41
E-mail: rio@urfu.ru

Отпечатано в Издательско-полиграфическом центре УрФУ
620075, Екатеринбург, ул. Тургенева, 4
Тел.: 8 (343) 350-56-64, 350-90-13
Факс: 8 (343) 358-93-06
E-mail: press-urfu@mail.ru

Для заметок

Для заметок