Министерство образования Республики Беларусь
БЕЛОРУССКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Кафедра «Высшая математика №1»

СПЕЦИАЛЬНЫЕ ГЛАВЫ МАТЕМАТИКИ. ОСНОВЫ ТЕОРИИ ЧИСЕЛ. ОСНОВНЫЕ АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ

Учебное электронное издание

Минск БНТУ 2011

УДК 519.17 (075.8)

А в т о р ы:
В.И. Каскевич, Е.А. Федосик, Н.И. Чепелев

Р е ц е н з е н т ы :

М.М. Чуйко, кандидат физико-математических наук, ведущий научный сотрудник институт математики НАН РБ;
В.В. Павлов, кандидат физико-математических наук, доцент кафедры «Высшей математики №2» БНТУ

Пособие разработано в соответствии с рабочей программой курса «Специальные главы математики для специальности «Программное обеспечение информационных технологий»» ФИТР БНТУ. Изложены основные понятия по двум базовым разделам математики: теории чисел и основным алгебраическим структурам. Предлагаемый материал ставит своей целью помочь студентам овладеть твердыми знаниями математических основ, которые позволили бы им успешно ориентироваться в специальной литературе по данной тематике и на основании этого перейти к серьезным приложениям. Пособие будет полезно всем лицам, изучающим общий курс высшей математики, как очной, так и на заочной формах обучения.

Белорусский национальный технический университет
пр-т Независимости, 65, г. Минск, Беларусь
Тел. (017) 292-80-75
E-mail: mathematics1@bntu.by
Регистрационный №

ОГЛАВЛЕНИЕ

1. ОСНОВЫ ТЕОРИИ ЧИСЕЛ

1.1. Делимость целых чисел. Теорема о делении с остатком

Множество целых чисел Z является объединением трех множеств: множества натуральных чисел, множества чисел, противоположных натуральным и множества, состоящего из одного числа нуль: $Z = (\ldots,-3,-2,-1,0,1,2,3,\ldots)$. Это счетное множество. На множестве Z определены две алгебраические операции – сложение и умножение. Результат операции деления целого числа a на целое число $b \neq 0$ есть число рациональное и в редких случаях является целым. В общем случае справедлива

Теорема 1.1 (о делении с остатком). *Для любых целых чисел a и b,* $b \neq 0$, *существуют единственные целые числа* q *и* r, $0 \le r < |b|$, *такие, что* $a = b \cdot q + r$.

В этом равенстве r называют остатком от деления a на b, число q – неполным частным. Очевидно, $r = 0$ тогда и только тогда, когда b является делителем a, в этом случае q называют частным от деления a на b. Частное (неполное частное) и остаток легко находятся методом деления уголком.

Пример 1.1.

а) $a = -31, b = 4;$ тогда $q = -7, r = -3$,

б) $a = 20, b = -3;$ тогда $q = -6, r = 2$,

в) $a = 57, b = 6;$ тогда $q = 9, r = 3$.

Если в теореме 1.1 число $r = 0$, то есть $a = b \cdot q$, то говорят, что a делится на b и q (и пишут: $a : b, a : q$), что a является кратным чисел b и q, что b и q делят a, а также называют b и q делителями или множителями числа a.

Важной является следующая

Лемма 1.1. *Если в равенстве* $a_1 + a_2 + \ldots + a_n = b_1 + b_2 + \ldots + b_m$ *все слагаемые – целые числа и все, кроме, может быть, одного, делятся на целое d , то и это исключенное слагаемое делится на d.*

1.2. Наибольший общий делитель целых чисел. Алгоритм Евклида

Определение 1.1. *Если целые числа* $a_1, a_2, \ldots, a_n$ *делятся на целое число d, то d называют их общим делителем.*

Далее рассматриваются только положительные целые делители.

Определение 1.2. *Максимальный из общих делителей целых чисел* $a_1, a_2, \ldots, a_n$ *называется их наибольшим общим делителем и обозначается через* $НОД(a_1, a_2, \ldots, a_n)$.

Теорема 1.2. *Если* $a = b \cdot q + c$, *то* $НОД(a, b) = НОД(b, c)$.

Доказательство. Пусть $d = НОД(a, b)$ и $k = НОД(b, c)$. В силу леммы 1.1 из делимости a и b на d следует, что и c делится на d. Таким образом, d – общий делитель чисел b и c. Следовательно, k делится на d. Но из равенства

$a = b \cdot q + c$ следует, что a делится на k. Тогда и d делится на k. Так как d и k являются натуральными, то отсюда следует, что $d = k$.

По сути дела, кратным применением этой теоремы является алгоритм Евклида (III век до н.э.), который можно сформулировать в виде следующей теоремы:

Теорема 1.3. *Наибольший общий делитель целых a и b ($a > b$) равен последнему отличному от нуля остатку цепочки равенств:*

$$a = b \cdot q_1 + r_1;$$

$$b = r_1 \cdot q_2 + r_2;$$

$$r_1 = r_2 \cdot q_3 + r_3;$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$r_{n-2} = r_{n-1} \cdot q_n + r_n;$$

$$r_{n-1} = r_n \cdot q_{n+1};$$

т.е. $r_n = НОД(a, b)$.

Пример 1.2. С помощью алгоритма Евклида найти *НОД* (294, 30).

Решение. По теореме 1.3 $294=30 \cdot 9+24$; $30=24 \cdot 1+6$; $24=6 \cdot 4$. Следовательно, *НОД* (294, 30)=6.

Обратное применение цепочки равенств алгоритма Евклида приводит к равенству, которое называют соотношением Безу для наибольшего общего делителя целых чисел a и b.

Теорема 1.4. *Если $d = НОД(a, b)$, то существуют такие целые u и v, что выполняется соотношение $d = au + bv$.*

Пример 1.3. Из примера 1.2 следует

$6 = 30 + 24(-1) = 30 + (-1)(294 + 30(-9)) = 294(-1) + 30 \cdot 10$, т.е. $u = -1, v = 10$.

1.3. Простые числа

Определение 1.3. *Натуральное число p, не равное единице, называется простым, если оно делится только на себя и на единицу, т.е. имеет только два делителя. Натуральное число, отличное от единицы и не являющееся простым, называется составным.*

Другими словами, натуральное число называется составным, если оно имеет более двух делителей. Число 1 не относится ни к простым, ни к составным числам, поскольку оно имеет лишь один делитель. Наименьшим простым числом является число 2. Это единственное четное простое число. Остальные простые числа являются нечетными.

Таким образом, множество натуральных чисел разбивается на три подмножества. Первое из них содержит только одно число – 1, второе образует простые числа, а третье – составные числа. Каждое натуральное число попадает в одно и только в одно из этих подмножеств; эти подмножества попарно не пересекаются (не имеют общих элементов).

Очевидно, справедлива

Теорема 1.5. *Всякое натуральное число* $n > 1$ *либо является простым числом, либо имеет простой делитель.*

Очевидно, множество простых чисел, не превосходящих некоторого числа *n*, будет конечным (как подмножество конечного множества). Проще всего найти эти простые числа методом, который впервые был предложен древнегреческим ученым Эратосфеном Киренским (ок. 276 – 194 г.г. до н.э.), и получил название «решето Эратосфена». Рассмотрим алгоритм этого метода. Пусть требуется найти все простые числа, не превосходящие числа *n*. Выпишем подряд все числа от 1 до n: $1,2,3,\ldots,n$. Первым здесь стоит число 1. Как известно, оно не является простым. Вычеркнем это число. Следующее число 2. Это простое число. Оставляем его и вычеркнем все числа, кратные 2. Для этого достаточно вычеркнуть каждое второе число, начиная счет с 3. Первым не вычеркнутым числом будет 3. Это простое число. Оставляем его и вычеркнем все числа, кратные трем, т.е. каждое третье число, начиная счет с 4. При счете необходимо учитывать и ранее вычеркнутые числа, поэтому некоторые числа вычеркиваются второй раз, такими числами будут 6, 12, 18, …. После этой операции первым не вычеркнутым, а значит и простым, будет число 5. Оставляем это число и вычеркиваем все числа, кратные 5, т.е. каждое пятое число, начиная счет с 6. Затем переходим к следующему не вычеркнутому числу (таким будет 7), производим аналогичные действия (вычеркивая все числа, кратные 7, т.е. каждое седьмое число, начиная счет с 8) и так далее. Таким способом мы вычеркнем все составные числа, останутся лишь простые числа. В таблице 1.1 приведены результаты указанных действий для случая $n = 70$; вычеркнутые числа отмечены черточкой над ними. По этой таблице находим все простые числа от 1 до 70. Их всего 19: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67.

Таблица 1.1

$\overline{1}$	2	3	$\overline{4}$	5	$\overline{6}$	7	$\overline{8}$	$\overline{9}$	$\overline{10}$
11	$\overline{12}$	13	$\overline{14}$	$\overline{15}$	$\overline{16}$	17	$\overline{18}$	19	$\overline{20}$
$\overline{21}$	$\overline{22}$	23	$\overline{24}$	$\overline{25}$	$\overline{26}$	$\overline{27}$	$\overline{28}$	29	$\overline{30}$
31	$\overline{32}$	$\overline{33}$	$\overline{34}$	$\overline{35}$	$\overline{36}$	37	$\overline{38}$	$\overline{39}$	$\overline{40}$
41	$\overline{42}$	43	$\overline{44}$	$\overline{45}$	$\overline{46}$	47	$\overline{48}$	$\overline{49}$	$\overline{50}$
$\overline{51}$	$\overline{52}$	53	$\overline{54}$	$\overline{55}$	$\overline{56}$	$\overline{57}$	$\overline{58}$	59	$\overline{60}$
61	$\overline{62}$	$\overline{63}$	$\overline{64}$	$\overline{65}$	$\overline{66}$	67	$\overline{68}$	$\overline{69}$	$\overline{70}$

Метод Эратосфена получил название решета по следующим причинам. Древние греки рабочие записи вели заостренной палочкой на восковых дощечках. Такой палочкой Эратосфен прокалывал те места, где были написаны составные числа. После этого восковая дощечка становилась похожей на решето. Применяя метод Эратосфена, как бы отсеивают, пропускают через решето все составные числа и оставляют только простые.

К настоящему времени разработан достаточно большой цикл алгоритмов проверки числа на простоту. Лишь в 2002 г. группа индийских математиков

конструктивно установила существование полиномиального алгоритма распознавания простоты натурального числа.

Теорема 1.6 (Евклид, III в. до н.э.). *Множество простых чисел является бесконечным.*

Доказательство. Предположим противное, т.е. множество простых чисел конечно и выпишем их все: $P_1, P_2, \ldots, P_n$, $P_1 = 2, P_2 = 3, P_3 = 5, \ldots$. Произведение всех простых чисел обозначим буквой $P = P_1 \cdot P_2 \cdot \ldots \cdot P_n$ и рассмотрим число $P+1$. Число $P+1$ больше каждого из чисел $P_1, P_2, \ldots, P_n$; оно не может быть простым (в силу предположения). Следовательно, число $P+1$ делится хотя бы на одно простое число P_k (k – одно из чисел $(1,2,\ldots,n)$). Число P также, очевидно, делится на простое число P_k. В силу леммы 1.1 число 1 также должно делиться на P_k, что возможно лишь в случае $P_k = 1$, а это противоречит предположению (P_k – простое число, поэтому $P_k \neq 1$). Полученное противоречие с предположением доказывает теорему.

Определение 1.4. *Всякое натуральное число, которое делится одновременно на натуральные числа a и b, называется общим кратным этих чисел. Наименьшее из таких чисел называют наименьшим общим кратным чисел a и b.*

Теорема 1.7. *Наименьшее общее кратное двух взаимно простых чисел равно их произведению.*

Значение простых чисел заключается в том, что они по теореме 1.5 являются составными кирпичиками всех натуральных чисел. Распределение простых чисел среди чисел натурального ряда достаточно не предсказуемо, о чем свидетельствуют следующие две теоремы.

Теорема 1.8 (Чебышев, 1852). *Между натуральными числами k и* $2k$, $k > 1$, *обязательно найдутся простые.*

Теорема 1.9. *Для всякого натурального n существует отрезок* $[k, k+n]$ *натурального ряда, все числа которого составные.*

Доказательство. Действительно, все следующие числа составные: $(n+2)!+2; (n+2)!+3; \ldots; (n+2)!+(n+2)$. Здесь $k! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot k$.

При рассмотрении все больших и больших натуральных чисел простые числа встречаются все реже. Всего имеется 168 простых чисел между 1 и 1000, 135 – между 1000 и 2000, 127 – между 2000 и 3000, 120 – между 3000 и 4000, 119 – между 4000 и 5000. Тем не менее, простых чисел бесконечное множество.

В конце XVIII в. была серьезно поставлена проблема определения функции $\pi(x)$, выражающей число простых чисел от 2 до x. Первыми приближенную формулу получили независимо друг от друга Лежандр (1752–1833) и Гаусс, но доказательств этих формул они не представили. Гаусс в 15 лет высказал гипотезу, что $\pi(x)$ подчинена достаточно равномерному закону. Первые теоретические результаты по функции $\pi(x)$ получил П.Л. Чебышев.

Теорема 1.10 (Адамар, Валле-Пуссен, 1896).

$\pi(x) \approx \dfrac{x}{\ln x}$.

Любопытным фактом является

Теорема 1.11 (Эйлер, 1737). *Ряд* $\dfrac{1}{2}+\dfrac{1}{3}+\dfrac{1}{5}+\dfrac{1}{7}+\ldots$ *из обратных простых чисел – расходящийся.*

Еще Евклид интересовался простыми числами специального вида:

$$M_p = 2^p - 1\ , \qquad (1.1)$$

где p – простое число. Если начать вычислять по этой формуле, то увидим, что не все числа оказываются простыми. Например, при $p = 2,3,5,7$ получаем соответственно $M_2 = 3, M_3 = 7, M_5 = 31, M_7 = 127$, а при $p = 11$ – составное число $M_{11} = 2047 = 23 \cdot 89$.

Простые числа вида (1.1) *называют числами Мерсенна*. Свое название они получили в честь французского ученого Марена Мерсенна (1588–1648). К середине XVIII в. было известно семь простых чисел Мерсенна, соответствующих значениям $p = 2,3,5,7,13,17,19$.

В 1750 г. Леонард Эйлер (1707–1783) нашел восьмое простое число Мерсенна при $p = 31$. Лишь в 1883 г. русский математик-самоучка сельский священник Пермской губернии И.М. Первушин (1827–1900) вычислил новое простое число при $p = 61$:

$M_{61} = 2305843009213693951$.

Все указанные 9 простых чисел Мерсенна были вычислены с помощью только карандаша и бумаги. На конец XX века наибольшим известным простым числом было число $2^{6972593} - 1$. Проверка чисел Мерсенна на простоту производится гораздо проще (алгоритм Люка, см., например, [18], чем произвольных натуральных чисел. Поэтому они и попадают в категорию рекордных.

Обобщением теоремы 1.6 является

Теорема 1.12 (Дирихле, 1837). *Всякая арифметическая прогрессия* $\{a + b \cdot n\}$*, где* $НОД(a,b) = 1$*, содержит бесконечно много простых чисел.*

Доказательство требует мощных аналитических средств, а с точки зрения временных затрат – отдельного спецкурса.

К сожалению, больше в теории чисел аналогичных результатов нет. Попытки найти их составляют целые направления в теории чисел. Сформулируем несколько гипотез и открытых проблем (ОП) теории чисел в данном направлении.

ОП1. Бесконечно ли множество простых чисел Мерсенна? На начало 2005 г. известно 29 простых чисел Мерсенна.

ОП2. Бесконечно ли много простых чисел Ферма?

Числа вида

$$F_m = 2^{2^m} + 1, \qquad (1.2)$$

называют числами Ферма в честь выдающегося французского математика Пье-

ра Ферма (1601–1665). Ферма был уверен в том, что все числа вида (1.2) являются простыми. Он рассматривал следующие пять чисел: $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$. Эти числа действительно являются простыми, но уже следующее число Ферма $F_5 = 4294967297 = 641 \cdot 6700417$ оказывается составным. Лишь в 1732 г. Эйлер обратил на это внимание. Предпринимались усиленные попытки найти новые простые числа Ферма. Однако эти попытки оказались безуспешными – ни одного нового простого числа Ферма не было найдено. Некоторые математики склонны считать, что других таких простых чисел нет.

ОП3. Бесконечно ли много простых чисел-близнецов, то есть пар простых чисел вида $p, p+2$? Примерами чисел-близнецов являются пары чисел 5 и 7, 17 и 19, 29 и 31, 41 и 43, 59 и 61, 71 и 73, 101 и 103, 107 и 109, 1997 и 1999 и так далее. Отметим, что в 1919 году Брун доказал, что даже в случае бесконечности пар чисел-близнецов ряд из обратных к ним – сходящийся [23].

ОП4 (Проблема Эйлера). Бесконечно ли много простых чисел – значений полинома $x^2 + x + 41$? Эйлер заметил, что при $x = 0,1,\ldots,39$ полином дает простые числа. Однако уже $f(40) = 41^2$. Следующее утверждение снимает проблему поиска полиномов, принимающих только простые значения.

Теорема 1.13. *Никакая целая рациональная функция от x с целыми коэффициентами для всякого натурального x не будет равняться простому числу.*

1.4. Критерий взаимной простоты целых чисел

Определение 1.5. *Целые числа a и b называются взаимно простыми, если* $НОД(a,b) = 1$.

Это целые числа, не имеющие общих простых делителей. Развитием теоремы 1.4 (о соотношении Безу) является

Теорема 1.14 (критерий взаимной простоты целых чисел). *Целые числа a и b взаимно просты тогда и только тогда, когда существуют такие целые u и v, что выполняется равенство* $au + bv = 1$.

Доказательство. Необходимость утверждения, то есть существование требуемых целых чисел *u* и *v* доказана теоремой 1.4. Докажем достаточность утверждения методом от противного. Пусть выполняется равенство целых чисел $au + bv = 1$. Если числа *a* и *b* имеют общий делитель $d > 1$, то в силу леммы 1.1 число 1 должно делиться на *d*, что невозможно. Таким образом, предположение о существовании у чисел *a* и *b* общего делителя $d > 1$ следует отбросить. Следовательно, $НОД(a,b) = 1$, что и требовалось доказать.

Следствие. $НОД(ac,b) = 1$ *тогда и только тогда, когда* $НОД(a,b) = 1$, $НОД(c,b) = 1$.

Лемма 1.2. *Пусть произведение целых чисел ab делится на целое число c и* $НОД(a,c) = 1$. *Тогда b делится на c.*

Доказательство. Согласно критерию взаимной простоты целых чисел (теорема 1.14) имеет место равенство $au + cv = 1$ для подходящих целых чисел *u*

и v. Умножим это на число b. Получим равенство $abu + bcv = b$. Левая часть этого равенства делится на c. Следовательно, в силу леммы 1.1, и правая часть равенства – число b делится на c. Лемма доказана.

1.5. Основная теорема арифметики

Теорема 1.15. *Всякое целое число* $n > 1$ *однозначно раскладывается в произведение простых множителей:*

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_s . \tag{1.3}$$

Доказательство. Для малых значений n утверждение теоремы проверяется непосредственно. Пусть $n > 1$ и предположим, что утверждение теоремы верно для всех натуральных чисел, меньших n. Согласно теореме 1.5 число n либо является простым (тогда теорема доказана), либо делится на некоторое простое число p. Тогда $n = pm$ для натурального $m < n$. По предположению индукции число m раскладывается в произведение простых множителей. Таким образом, доказано существование разложения всякого натурального числа в произведение простых множителей.

Единственность разложения доказывается методом от противного. Предположим, что натуральное число n имеет два различных разложения в произведение простых множителей:

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_s = q_1 \cdot q_2 \cdot \ldots \cdot q_t . \tag{1.4}$$

Предположим, что $t \le s$. В силу леммы 1.1 левая часть этого равенства делится на q_1. Если $НОД(p_1, q_1) = 1$, то согласно лемме 1.2 произведение $p_2 \cdot p_3 \cdot \ldots \cdot p_s$ делится на q_1. Рассуждая и далее аналогичным образом, найдем некоторый множитель p_k, делящийся на q_1, то есть найдем $p_k = q_1$. Сократим равенство (1.4) на этот общий множитель. Аналогично рассуждаем с $q_2 \cdot q_3 \cdot \ldots \cdot q_t$. В конце концов, придем к соотношению

$$p_1^* \cdot p_2^* \cdot \ldots \cdot p_{s-t}^* = 1, \tag{1.5}$$

где $p_i^*, 1 \le i \le s - t$ – не сократившиеся простые множители левой части равенства (1.4). Но единица не может делиться ни на одно из простых чисел. Следовательно, $s = t$, и на самом деле равенство (1.5) имеет вид $1 = 1$. Это и означает единственность разложения в произведение простых множителей с точностью до порядка следования этих множителей. Теорема доказана.

Если в равенстве $n = p_1 \cdot p_2 \cdot \ldots \cdot p_s$ собрать одинаковые множители, то получим следующее каноническое разложение целого числа:

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_t^{r_t} .$$

Пример 1.4. a) $9702 = 2 \cdot 3^2 \cdot 7^2 \cdot 11$; b) $341887 = 7 \cdot 13^2 \cdot 17^2$;

c) $2^{12} - 1 = 4095 = 3^2 \cdot 5 \cdot 7 \cdot 13$.

По каноническому разложению целых чисел легко находится их наибольший общий делитель, наименьшее общее кратное, решаются иные задачи.

Пример 1.5. Найти $НОД(a, b)$ и $НОК(a, b)$, если a) $a = 126, b = 330$. Раз-

ложим эти числа на простые множители: $126 = 2 \cdot 3^2 \cdot 7; 330 = 2 \cdot 3 \cdot 5 \cdot 11$. $НОД(a,b) = 2 \cdot 3 = 6$, $НОК(a,b) = 2 \cdot 3^2 \cdot 57 \cdot 11 = 6930$.

б) $a = 525, b = 385; 525 = 3 \cdot 5^2 \cdot 7; 385 = 5 \cdot 7 \cdot 11$; $НОД(a,b) = 5 \cdot 7 = 35$; $НОК(a,b) = 3 \cdot 5^2 \cdot 7 \cdot 11 = 5775$.

Следует отметить, что теорема 1.15 – это теорема существования. Она не дает метода факторизации натурального числа в произведение простых сомножителей. Поиск эффективного метода факторизации целых чисел оказался сложной алгоритмической проблемой, причем более сложной, чем распознавание простоты натурального числа. Ни один из имеющихся алгоритмов не является полиномиальным относительно n. Безуспешные и настойчивые поиски такого алгоритма приводят к убеждению, что задача факторизации целых чисел имеет экспоненциальную сложность. Данное обстоятельство, в частности, обеспечивает стойкость криптосистемы RSA.

1.6. Сравнения

Теорема 1.16. *Пусть m – натуральное число, $m > 1$. Для любых целых чисел a и b следующие условия равносильны:*

1) a и b имеют одинаковые остатки от деления на m;

2) $a - b$ делится на m, то есть $a - b = mq$ для подходящего целого q;

3) $a = b + mq$ для некоторого целого q.

Доказательство проводится по схеме: $1) \Rightarrow 2) \Rightarrow 3) \Rightarrow 1)$. Из условия 1 следует условие 2: если $a = mq_1 + r, b = mq_2 + r$, то $a - b = m(q_1 - q_2)$, что означает делимость $a - b$ на m. Из условия 2 $a - b = mq$ следует $a = b + mq$. Докажем, что из $3) \Rightarrow 1)$. Если $b = ms + r$, то из равенства $a = b + mq$ получаем: $a = ms + r + mq = m(s + q) + r$, т.е. a и b имеют одинаковые остатки от деления на m. Теорема доказана.

Определение 1.6. *Целые числа a и b называются сравнимыми по модулю m, если они удовлетворяют одному из условий теоремы 1.16. Этот факт обозначают формулой $a \equiv b(\mathrm{mod}\, m)$ или $a \equiv b(m)$. Данное соотношение между целыми числами называют сравнением по модулю m.*

Пример 1.6. $-4 \equiv 2(\mathrm{mod}\, 3) \equiv 5(\mathrm{mod}\, 3) \equiv 8(\mathrm{mod}\, 3) \equiv 14(\mathrm{mod}\, 3)$.

Основные свойства сравнений.

Свойство 1. *Пусть $a \equiv b(\mathrm{mod}\, m)$. Тогда $(a \pm c) = (b \pm c)(\mathrm{mod}\, m)$ для всякого целого c, то есть к обеим частям сравнения можно добавить (или вычесть из обеих частей) одно и то же число.*

Доказательство. $a \equiv b(\mathrm{mod}\, m)$ тогда и только тогда, когда $a - b = mq$ для подходящего целого q. Следовательно, $(a + c) - (b + c) = mq$, то есть $(a + c)$ и $(b + c)$ сравнимы друг с другом по модулю m.

Свойство 2. *Сравнения можно почленно складывать и вычитать: если $a \equiv b(\mathrm{mod}\, m), c \equiv d(\mathrm{mod}\, m)$, то $(a + c) \equiv (b + d)(\mathrm{mod}\, m); (a - c) \equiv (b - d)(\mathrm{mod}\, m)$.*

Доказательство аналогично предыдущему: если $a-b=mq; c-d=mt$, то $(a+c)-(b+d)=m(q+t)$. Следовательно, $(a+c)=(b+d)(\mathrm{mod}\, m)$.

Свойство 3. *Сравнения можно почленно перемножать: если* $a \equiv b(\mathrm{mod}\, m), c \equiv d(\mathrm{mod}\, m)$, *то* $ac \equiv bd(\mathrm{mod}\, m)$.

Доказательство. Согласно третьему условию теоремы 1.16 $a=b+mq; c=d+mw$ для подходящих целых q и w. Тогда $ac=bd+m(qd+bw+mqw)$. Согласно тому же третьему условию, это означает, что $ac \equiv bd(\mathrm{mod}\, m)$.

Свойство 4. *Сравнения можно почленно возводить в натуральную степень: если* $a \equiv b(\mathrm{mod}\, m)$, *то* $a^n \equiv b^n(\mathrm{mod}\, m)$.

Доказательство непосредственно следует из доказанного свойства 3.

Свойство 5. *Если в сравнении* $a \equiv b(\mathrm{mod}\, m)$ *числа a, b, m имеют общий множитель d, то на него сравнение можно сократить:* $(a/d) \equiv (b/d)(\mathrm{mod}(m/d))$.

Доказательство. Пусть $a=da_1, b=db_1, m=dm_1$. Согласно третьему условию теоремы 1.16 $a=b+mq$, то есть $da_1=db_1+dm_1q$. Сократив данное равенство на d, получим равенство $a_1=b_1+m_1q$, означающее сравнимость целых a_1 и b_1 по модулю m_1.

Свойство 6. *Сравнение можно сократить на общий множитель, взаимно простой с модулем: если* $a=da_1, b=db_1, НОД(d,m)=1$, *то из сравнения* $da_1 \equiv db_1(\mathrm{mod}\, m)=1$ *следует сравнимость* a_1 *и* b_1 *по модулю m:* $a_1 \equiv b_1(\mathrm{mod}\, m)$.

Доказательство. По второму условию теоремы 1.16 $da_1-db_1=mv$ для подходящего целого v. Следовательно, произведение mv делится на d. Поскольку $НОД(d,m)=1$, то согласно лемме 1.2 целое v делится на d: $v=dv_1$. Следовательно, $a_1=b_1+mv_1$, то есть $a_1 \equiv b_1(\mathrm{mod}\, m)$, что и требовалось доказать.

Свойства 1–6 относятся к арифметическим свойствам сравнений. Сравнимость целых чисел по данному модулю m определяет бинарное отношение $R_{\mathrm{mod}\, m}$ на множестве целых чисел: два целых числа находятся в отношении $R_{\mathrm{mod}\, m}$, тогда и только тогда, когда они сравнимы друг с другом по модулю m. Легко проверяются следующие свойства названного бинарного отношения.

Свойство 7. *Рефлексивность:* $a \equiv a(\mathrm{mod}\, m)$ *для любого целого a и всякого натурального* $m>1$.

Свойство 8. *Симметричность: если* $a \equiv b(\mathrm{mod}\, m)$, *то* $b \equiv a(\mathrm{mod}\, m)$.

Свойство 9. *Транзитивность: если* $a \equiv b(\mathrm{mod}\, m), b \equiv c(\mathrm{mod}\, m)$, *то* $a \equiv c(\mathrm{mod}\, m)$.

Свойства 7–9 означают, что отношение сравнимости на множестве целых чисел Z есть отношение эквивалентности. Это означает, что Z разбивается на непересекающиеся классы попарно сравнимых друг с другом целых чисел по данному модулю. Каждый класс сравнимых друг с другом целых чисел характеризуется общими свойствами представителей этого класса. Например, все они имеют один и тот же остаток от деления на модуль; все они в силу теоремы

1.2 имеют одинаковый наибольший общий делитель с этим модулем.

1.7. Кольцо классов вычетов

При делении целых чисел на натуральное целое $m>1$ существует m различных остатков: $0,1,2,\ldots,m-1$. Соответственно этим остаткам множество Z разбивается на m непересекающихся классов сравнимых друг с другом чисел, имеющих, как отмечено в 1.6, один и тот же остаток. В соответствии с остатками от деления на m эти классы будем обозначать через $\overline{0},\overline{1},\overline{2},\ldots,\overline{m-1}$. Таким образом, класс $\bar{i}=\{mq+i|q\in Z\}$ для каждого целого $i=0,1,2,\ldots,m-1$. Любой представитель класса однозначно определяет свой класс, то есть для каждого $mq+i$ класс $\overline{mq+i}=\bar{i}$. Поскольку остаток – на латыни residu – переводится на русский как вычет, то множество всех классов по данному модулю сравнимых друг с другом чисел называют множеством классов вычетов по модулю и обозначают через Z/mZ. В силу сказанного $Z/mZ=\{\overline{0},\overline{1},\overline{2},\ldots,\overline{m-1}\}$ – множество из m элементов.

Определим операции сложения на Z/mZ. Полагаем суммой $\bar{k}\oplus\bar{l}$ такой единственный класс $\bar{z}$ из Z/mZ, в который попадают все суммы k_1+l_1 и k_2+l_2 для $k_1,k_2\in\bar{k}, l_1,l_2\in\bar{l}$, а произведением $\bar{k}\bar{l}$ – тот класс из Z/mZ, в который попадают произведения $\bar{k}\cdot\bar{l}$ для $k\in\bar{k}, l\in\bar{l}$.

Поскольку сложение и умножение в Z/mZ однозначно определяются умножением представителей классов, то свойства операций сложения и умножения целых чисел справедливы и в Z/mZ:

1) $\bar{k}\oplus\bar{l}=\bar{l}\oplus\bar{k}; \bar{l}\bar{k}=\bar{k}\bar{l}$ – коммутативность;

2) $\bar{k}\oplus(\bar{l}\oplus\bar{r})=(\bar{k}\oplus\bar{l})\oplus\bar{r}; \bar{k}(\bar{l}\bar{r})=(\bar{k}\bar{l})\bar{r}$ – ассоциативность;

3) существует нейтральный элемент: $\bar{k}\oplus\overline{0}=\bar{k}; \bar{k}\cdot\overline{1}=\bar{k}$;

4) для всякого $\bar{k}\in Z/mZ$ существует единственный класс $\bar{l}$ такой, что $\bar{k}\oplus\bar{l}=\overline{0}$, им является $\bar{l}=\overline{m-k}$;

5) $(\bar{k}\oplus\bar{l})\bar{r}=(\bar{k}\bar{r})\oplus(\bar{l}\bar{r})$ – дистрибутивность.

Далее операции сложения и умножения в этом кольце будем обозначать стандартными символами «+» и «–».

Таким образом, Z/mZ является коммутативным кольцом с единицей.

Определение 1.7. *Элемент $\bar{k}\in Z/mZ$ называется обратимым, если найдется такой класс $\bar{l}\in Z/mZ$, что $\bar{k}\cdot\bar{l}=\overline{1}$. Тогда класс $\bar{l}$ называют обратным к классу $\bar{k}$.*

Из ассоциативности умножения в кольце Z/mZ вытекает, что если $\bar{k}$ обратимый класс, то обратный класс определен однозначно.

Лемма 1.3. *Пусть $\bar{k}\in Z/mZ$ такой класс, что $НОД(k,m)=1$. Тогда*

1) для каждого $\bar{l}\neq\overline{0}$ произведение $\bar{k}\bar{l}\neq\overline{0}$;

2) $\bar{k}\cdot\bar{l}_1\neq\bar{k}\cdot\bar{l}_2$, если $\bar{l}_1\neq\bar{l}_2$;

3) отображение $f:\bar{x}\to\bar{k}\bar{x}$ *инъективно и, следовательно, биективно на множестве* Z/mZ *(на множестве ненулевых элементов из* Z/mZ*);*

4) $\bar{k}$ *– обратимый класс в кольце* Z/mZ.

Замечание. Поскольку, согласно условию леммы 1.3, $НОД(k,m)=1$, то по критерию взаимной простоты (теорема 1.14) существуют такие целые $u,v\in Z$, что $ku+mv=1$. Тогда $\bar{1}=\bar{k}\bar{u}+\bar{m}\bar{v}=\bar{k}\bar{u}$. Следовательно, $\bar{u}$ – обратный к $\bar{k}$ класс.

Лемма 1.4. *Пусть* $\bar{k}\in Z/mZ$ *такой класс, что* $НОД(k,m)=d>1$. *Тогда*

1) существует класс $\bar{l}\neq\bar{0}$, *что* $\bar{k}\bar{l}=\bar{0}$;

2) существуют классы $\bar{l}_1\neq\bar{l}_2$, *такие, что* $\bar{k}\cdot\bar{l}_1=\bar{k}\cdot\bar{l}_2$;

3) для всех $\bar{l}\neq\bar{0}$ *произведение* $\bar{k}\cdot\bar{l}\neq\bar{1}$, *то есть класс* $\bar{l}$ *необратим в кольце* Z/mZ.

Теорема 1.17. *Класс* $\bar{k}$ *из кольца* Z/mZ *обратим тогда и только тогда, когда* $НОД(k,m)=1$. *Обратный класс также обратим. Произведение обратимых классов есть обратимый класс.*

Следствие. *Если* $m=p$ *– простое число, то в кольце* Z/mZ *каждый ненулевой класс обратим.*

Поскольку Z/mZ состоит из конечного множества элементов, то сложение и умножение можно задавать поэлементно в виде таблиц.

Пример 1.7. Напишем таблицы сложения и умножения в кольце $Z/3Z$:

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

Из таблицы умножения непосредственно видно, что классы $\bar{1}$ и $\bar{2}$ обратны сами себе, то есть обратимы все ненулевые классы $Z/3Z$ в полном соответствии с теоремой 1.17.

1.8. Малая теорема Ферма

Такое название в теории чисел и ее приложениях носит следующая

Теорема 1.18. *Пусть* p *– простое число и целое число* a *не делится на* p. *Тогда* $a^{p-1}\equiv 1(\mathrm{mod}\ p)$.

Доказательство. Согласно лемме 1.3 равны произведения $(\bar{a}\cdot\bar{1})\cdot(\bar{a}\cdot\bar{2})\cdot\ldots\cdot(\bar{a}\cdot\overline{n-1})=\bar{1}\cdot\bar{2}\cdot\ldots\cdot(\overline{n-1})$. Сократим это равенство на $\bar{2}\cdot\bar{3}\cdot\ldots\cdot(\overline{n-1})$. Получим $\bar{a}^{p-1}=\bar{1}$. Это означает, что $a^{p-1}\equiv 1(\mathrm{mod}\ p)$.

Следствие 1. *В кольце* Z/mZ *с простым* p *обратным к классу* $\bar{k}\neq\bar{0}$ *является класс* $\bar{k}^{p-2}$.

Пример 1.8. а) Пусть $p=3, a=4$. Тогда по теореме 1.18 $4^{3-1}=1+3\cdot 5$,

т.е. $16 = 1 + 15$, т.е. $16 \equiv 1 (\mathrm{mod}\, 3)$; б) $p = 5, a = 9; 9^{5-1} = 1 + 5 \cdot 1312$, т.е. $6561 = 1 + 6560$, т.е. $6561 \equiv 1 (\mathrm{mod}\, 5)$.

Замечание. В соответствии с замечанием к лемме 1.3 класс $\bar{k}^{-1}$ можно найти обратной прогонкой алгоритма Евклида. Следствие дает конкурентный способ нахождения обратного класса. Он кажется громоздким, но свойства сравнений позволяют достаточно быстро вычислить остаток от деления k^{p-2} на p. Во-первых, от k можно перейти к остатку от деления k на p. Поэтому можно считать, что $1 < k < p$. Требуемую степень можно вычислить за $0(\log_2(p-2))$ умножений. Для этого можно представить $p-2$ в двоичной системе счисления.

Пример 1.9. Найти остаток от деления 28^{21} на 17.

Решение. Двоичная запись $21 = 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = (10101) = 16 + 4 + 1$. Значит, для любого натурального a величина $a^{21} = a^{2^4} \cdot a^{2^2} \cdot a^{2^0}$; здесь $28^{21} = 28^{16} \cdot 28^4 \cdot 28^1$. Далее, $28 = 11 + 17 \cdot 1$, т.е. $28^1 \equiv 11 (\mathrm{mod}\, 17)$, $28^2 \equiv 11^2 (\mathrm{mod}\, 17) \equiv 2 (\mathrm{mod}\, 17)$ (т.к. $11^2 = 121 = 2 + 17 \cdot 7$), $28^4 \equiv$ $\equiv 2^2 (\mathrm{mod}\, 17) \equiv 4 (\mathrm{mod}\, 17)$, $28^8 \equiv 4^2 (\mathrm{mod}\, 17) \equiv 16 (\mathrm{mod}\, 17)$; $28^{16} \equiv 16^2 (\mathrm{mod}\, 17) \equiv$ $\equiv 256 (\mathrm{mod}\, 17) \equiv 1 (\mathrm{mod}\, 17)$ (т.к. $256 = 1 + 17 \cdot 15$). Таким образом, $28^{21} \equiv$ $\equiv 11 \cdot 4 \cdot 1 (\mathrm{mod}\, 17) \equiv 44 (\mathrm{mod}\, 17) \equiv 10 (\mathrm{mod}\, 17)$ (т.к. $44 = 10 + 17 \cdot 2$).

Ответ: остаток от деления 28^{21} на 17 равен 10.

Следствие 2. *Если* $a^{m-1} \neq 1 (\mathrm{mod}\, m)$ *для некоторого натурального a,* $1 < a < m-1$, *то число m – составное.*

Этот факт часто используется в качестве теста проверки числа на простоту. Он позволяет установить наличие множителей данного числа m, не находя ни одного из таких множителей.

Замечание. Из теста выброшено число $m-1$, поскольку в силу формулы бинома Ньютона $(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k$ для $a = m, b = -1, n = m-1$.

$$(m-1)^{m-1} = \sum_{k=0}^{n} C_{m-1}^k m^{m-k-1} (-1)^k = m^{m-1} - C_{m-1}^1 m^{m-2} + C_{m-1}^2 m^{m-3} - \ldots +$$

$$+ (-1)^k C_{m-1}^k m^{m-k-1} - \ldots + C_{m-1}^{m-2} m + (-1)^{m-1} =$$ (если m – простое, то оно нечетное – т.к. единственное простое четное число – 2; отсюда $(-1)^{m-1} = 1$) $=$

$$= m\left(m^{m-2} - C_{m-1}^1 m^{m-3} + \ldots + (-1)^k C_{m-1}^{m-k-2} - \ldots + C_{m-1}^m\right) + 1,$$ т.е. $(m-1)^{m-1} = 1 + mq$, где q – выражение, стоящее в скобках. Это означает, что $(m-1)^{m-1} \equiv 1 (\mathrm{mod}\, m)$.

Определение 1.8. *Нечетное натуральное число n называется псевдопростым по основанию b для некоторого целого* $b, 1 < b < n-1$, *если* $b^{n-1} \equiv 1 (\mathrm{mod}\, n)$.

Выдающийся немецкий математик и философ Готфрид Вильгельм Лейбниц (1646–1716) полагал, что псевдопростые числа на самом деле просты и использовал для проверки $b = 2$. Действительно, при $b = 2, n = 5$, $2^4 = 16 = 1 + 5 \cdot 3$,

т.е. $2^{5-1} \equiv 1(\mathrm{mod}\,5)$; $n = 7, 2^6 = 64 = 1 + 7 \cdot 9$, т.е. $2^{7-1} \equiv 1(\mathrm{mod}\,7)$; $n = 9, 2^8 = 256 = 1 + 3 \cdot 85$, т.е. $2^{9-1} \neq 1(\mathrm{mod}\,9)$; $n = 11, 2^{10} = 1024 = 1 + 1023 = 1 + 11 \cdot 93$, т.е. $2^{11-1} \equiv 1(\mathrm{mod}\,11)$ и так далее.

Однако существует контрпример: $2^{340} \equiv 1(\mathrm{mod}\,341)$, хотя $341 = 11 \cdot 31$ – составное число. Заметим также, что $3^{340} \equiv 56(\mathrm{mod}\,341)$.

Определение 1.9. *Нечетное натуральное число называется числом Кармайкла, если оно составное и псевдопростое по всем основаниям b.*

В 1912 г. Р.Д. Кармайкл впервые опубликовал примеры таких чисел (15 чисел), в частности, привел наименьшее из них $561 = 3 \cdot 11 \cdot 17$. Позже выяснилось, что характеризация чисел Кармайкла была получена 15-ю годами ранее А. Корселтом.

Теорема 1.19 (Корселта). *Нечетное натуральное число n является числом Кармайкла тогда и только тогда, когда для каждого его простого делителя p выполнены следующие два условия:*

1) n не делится на p^2;

2) $n-1$ делится на $p-1$.

Числа Кармайкла встречаются довольно редко. Например, между 1 и 10^9 имеется 50847534 простых чисел и 646 чисел Кармайкла. Тем не менее справедлива

Теорема 1.20 (Альфорд, Гранвиль, Померанц (1994)). *Чисел Кармайкла бесконечно много.*

1.9. Функция Эйлера и теорема Эйлера

Определение 1.10. *Функция Эйлера – функция $\varphi(m)$ натурального аргумента m, которая каждому натуральному числу $m > 1$ ставит в соответствие количество натуральных чисел, меньших m и взаимно простых с m.*

Эта функция обладает рядом свойств, облегчающих вычисление ее значений.

Свойство 1. $\varphi(p) = p - 1$ *для каждого простого числа p.*

Свойство 2. $\varphi(p^n) = p^n - p^{n-1}$ *для каждого простого числа p и для произвольного натурального* $n \geq 1$.

Свойство 3. *Если* $НОД(n, m) = 1$, *то* $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$.

Свойство 4. *Если* $n = p_1^{S_1} \cdot p_2^{S_2} \cdot \ldots \cdot p_t^{S_t}$ *– каноническое разложение числа n, то*

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

Пример 1.10. Найти $\varphi(m)$.

а) $\varphi(13)$. По свойству 1 $\varphi(13) = 13 - 1 = 12$.

б) $\varphi(8)$. По свойству 2 $\varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 4$. Действительно, взаимно

простых чисел, меньших 8, ровно 4: 1, 3, 5, 7.

в) $\varphi(15)$. По свойству 3 $\varphi(15)=\varphi(3\cdot 5)=\varphi(3)\cdot\varphi(5)=$(свойство 1) $=(3-1)(5-1)=2\cdot 4=8$. Действительно, число взаимно простых чисел, меньших 15, равно 8: 1, 2, 4, 7, 8, 11, 13, 14.

г) $\varphi(300)$. По свойству 4

$$\varphi(300)=\varphi\left(2^2\cdot 3\cdot 5^2\right)=300\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=300\cdot\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5}=80.$$

Пример 1.11. Из теоремы 1.17 следует, что в кольце Z/mZ имеется в точности $\varphi(m)$ обратимых классов. Например, $\varphi(12)=4$. Значит, в кольце $Z/12Z$ имеется ровно 4 обратимых элемента. Непосредственная проверка показывает, что этими классами являются $\overline{1},\overline{5},\overline{7},\overline{11}$.

Теорема 1.21 (*Эйлера*). *Если для целого числа a и натурального m* $НОД(a,m)=1$, *то* $a^{\varphi(m)}\equiv 1(\mathrm{mod}\, m)$.

Доказательство аналогично доказательству малой теоремы Ферма.

Следствие. *В кольце Z/mZ с составным m всякий обратимый элемент $\overline{k}$ обладает свойствами:*

1) $\overline{k}^{\varphi(m)}=1$;

2) обратным к $\overline{k}$ является класс $\overline{k}^{\varphi(m)-1}$.

2. ОСНОВНЫЕ АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ

2.1. Понятие группы

Определение 2.1. *Пусть X – непустое множество. Если на X задана одна или несколько алгебраических операций, то говорят, что X есть алгебраическая система с данными операциями.*

Из всех алгебраических операций наиболее применимыми оказались бинарные.

Определение 2.2. *Бинарной алгебраической операцией на множестве X называется всякое правило, по которому каждой упорядоченной паре (x,y) элементов $x,y\in X$ ставится в соответствие один вполне определенный элемент z из X.*

Обычно операции обозначаются знаками ∗, x, ·, +, – и т.п. Воспользуемся первым из обозначений операций. Тот факт, что элемент *z* множества *X* является результатом бинарной операции ∗ над элементами $x,y\in X$ в указанном порядке обозначают равенством $z=x*y$.

Пример 2.1. (*Z*, +, ·) – алгебраическая система целых чисел с операциями сложения и умножения, называемая кольцом целых чисел.

Алгебраические системы различают по операциям и свойствам этих операций.

Определение 2.3. *Алгебраическая система* (*X*, ∗) *с одной алгебраической*

операцией $*$ на множестве X называется группоидом. Если у группоида $(X, *)$ *операция $*$ ассоциативна: $a*(b*c)=(a*b)*c$, то такую алгебраическую систему называют полугруппой. Моноидом* $(X, *)$ *называют полугруппу с единицей или нейтральным элементом, т.е. таким элементом n, что $n*x=x*n=x$ для каждого $x \in X$.*

Пример 2.2. Алгебраическая система $(N, -)$ – множество натуральных чисел с операцией вычитания – группоид, $(N, +)$ – множество натуральных чисел с операцией сложения – полугруппа, $(N, \cdot)$ – множество натуральных чисел с операцией умножения – моноид. R_3 – множество всех свободных векторов трехмерного пространства с операцией векторного умножения – группоид, но не полугруппа, поскольку операция векторного умножения не ассоциативна: $\left[\vec{a},\left[\vec{b},\vec{c}\right]\right]=\vec{b}\cdot(\vec{a},\vec{c})-\vec{c}(\vec{a},\vec{b})$.

Лемма 2.1. *Если в полугруппе имеется нейтральный элемент, то он один.*

Доказательство. Если n и n' – два нейтральных элемента в полугруппе $(X, \cdot)$, то $n = n \cdot n' = n'$. Лемма доказана.

Определение 2.4. *Группой называется непустое множество G с определенной на нем бинарной алгебраической операцией $*$, которая обладает свойствами:*

1) ассоциативность: $a*(b*c)=(a*b)*c$ для любых $a,b,c \in G$;

2) существует нейтральный элемент (единица), то есть такой элемент $e \in G$, что $g*e=e*g=g$ для каждого $g \in G$;

3) каждый элемент $g \in G$ имеет обратный, то есть такой элемент $h \in G$, что $g*h=h*g=e$.

В силу леммы 2.1 в любой группе единица определяется однозначно. Это свойство дополняет

Лемма 2.2. *В любой группе элемент, обратный к каждому, определен однозначно.*

Пример 2.3. $(Q, +)$; $(R, +)$; $(C, +)$ множества всех рациональных, вещественных и комплексных чисел соответственно с операцией сложения являются так называемыми аддитивными группами.

Определение 2.5. *Абелевыми, или коммутативными, называют группы* $(G, *)$ *со свойством*

4) $a*b=b*a$ для произвольных $a,b \in G$.

По исторической традиции нейтральный элемент аддитивной группы называют нулем и обозначают 0, а обратный элемент к a – противоположным и обозначают через $-a$.

Пример 2.4. Мультипликативные группы – группы с операцией умножения: $(Q^*,\cdot), (R^*,\cdot), (C^*,\cdot)$, где $Q^* = Q \setminus \{0\}$, $R^* = R \setminus \{0\}$, $C^* = C \setminus \{0\}$.

По свойству 4 группы делятся на абелевы и не абелевы.

Пример 2.5. Абелевыми являются группы $(Z,+)$; $\{\pm,\cdot\}$; $(V_3,+)$ – множество классических векторов – направленных отрезков, выходящих из начала координат в пространство, с операцией *сложения векторов*.

$GL_n(R)$ – множество квадратных невырожденных матриц порядка $n>1$ с вещественными коэффициентами относительно операции матричного умножения является неабелевой группой.

По количеству элементов группы делятся на конечные и бесконечные.

Определение 2.6. *Порядком конечной группы называется количество элементов этой группы. Если G – конечная группа, то* $|G|$ *– ее порядок.*

Пример 2.6. Группа $(Z/nZ,\oplus)$ является конечной абелевой аддитивной группой из *n* элементов; в силу теоремы 1.7.1 множество $(Z/nZ)^*$ обратимых относительно умножения классов вычетов по модулю *n*, где *n* – натуральное число, большее единицы, образует группу порядка $\varphi(n)$.

2.2. Подгруппы

Определение 2.7. *Подгруппой в группе* $(G, \cdot)$ *называется всякое непустое подмножество H элементов множества G, которое в свою очередь является группой относительно той же операции.*

Тот факт, что *H* есть подгруппа группы *G* отмечают так: $H \le G$ или $H < G$, есть включение $H \subset G$ – строгое.

Пример 2.7. Аддитивные группы целых, рациональных, вещественных и комплексных чисел образуют систему подгрупп: $(Z, +)<(Q, +)<(R, +)<(C, +)$.

Подмножество всех целых чисел, делящихся на натуральное число $n>1$, образует подгруппу в группе целых чисел с операцией сложения. Эту подгруппу обозначают через $(nZ, +)$. Следовательно, имеют место бесконечные цепочки аддитивных подгрупп типа $(Z, +)>(2Z, +)>(4Z, +)>\ldots$.

Теорема 2.1 (критерий подгруппы). *Непустое подмножество H группы* $(G, \cdot)$ *является подгруппой тогда и только тогда, когда для произвольных элементов* $a,b \in H$ *имеет место включение* $a \cdot b^{-1} \in H$.

Пример 2.8. В силу критерия в любой группе *G* подмножество $\{e\}$ из одного нейтрального элемента *e* этой группы является подгруппой.

Определение 2.8. *Подгруппа H группы G называется собственной, если* $H \neq G$ *и* $H \neq \{e\}$.

Пример 2.9. С помощью критерия легко убедиться, что $SL_n(R)$ – подмножество квадратных матриц порядка *n* с определителем, равным 1, образуют подгруппу в $GL_n(R)$. Действительно, для произвольных матриц $A, B \in SL_n(R)$ по свойствам определителей $\det(B^{-1})=1$ и $\det(AB^{-1}) = \det A \cdot \det(B^{-1}) = 1$. Следовательно, $A, B^{-1} \in SL_n(R)$ и согласно критерию 2.3.1 $SL_n(R)$ является подгруппой в группе $GL_n(R)$.

2.3. Циклические группы и подгруппы

Теорема 2.2. *Пусть a – фиксированный элемент произвольной группы G. Пусть* $\langle a \rangle = \{a^0 = e, a, a^2, \ldots, a^{-1}, a^{-2}, \ldots\}$ *– множество всевозможных степеней элемента a. Тогда* $\langle a \rangle$ *– подгруппа группы G, причем абелева.*

Доказательство следует из критерия подгруппы: для произвольных $a^k, a^{-e} \in \langle a \rangle$ произведение $a^k \cdot a^{-e} = a^{k-e}$ принадлежит, очевидно, множеству $\langle a \rangle$.

Определение 2.9. *Подгруппа $\langle a \rangle$ из теоремы 2.2 называется циклической подгруппой группы G, порожденной элементом a. Если в группе G найдется такой элемент b, что $G = \langle b \rangle$, то такую группу называют циклической.*

Пример 2.10. Следующие группы являются циклическими: $(Z,+) = \langle 1 \rangle$; $(Z/nZ,+) = \langle \overline{1} \rangle$.

Теорема 2.3. *Пусть элемент $a \in G$ обладает свойством: $a^n = e$ для некоторого целого n и $a^k \neq e$ для всех целых $k, 1 \leq k < n$. Тогда циклическая подгруппа $\langle a \rangle$ имеет порядок n и $\langle a \rangle = \{a, a^2, \ldots, a^n = e\}$.*

Доказательство. Для целых $k, 1 \leq k < n, \left(a^k\right)^{-1} = a^{n-k}$.

Определение 2.10. *Величина n из теоремы 2.3 называется порядком элемента $a \in G$. Если же для элемента $a \in G$ такого n не существует, то говорят, что элемент имеет бесконечный порядок.*

Пример 2.11. Любое ненулевое целое число имеет бесконечный порядок в аддитивной группе целых чисел.

Пример 2.12. Возьмем матрицу $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL_2(R)$. Здесь $A^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$; $A^3 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$; …. Степени матрицы A попарно различны и образуют бесконечную последовательность. Определитель матрицы A равен $1 \neq 0$. $A^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$, $A^{-2} = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$, …. Таким образом, циклическая подгруппа, порожденная матрицей A в группе $GL_2(R)$, является бесконечной.

Пример 2.13. Матрица $H \in GL_2(R)$ вида $H = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ имеет степени $H^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$; $H^3 = \begin{pmatrix} 0 & -1 \\ 1 & 01 \end{pmatrix}$; $H^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E$ – единичная матрица. Согласно теореме 2.3 подгруппа $\langle H \rangle$ есть конечная подгруппа порядка четыре.

Теорема 2.4. *Всякая циклическая группа – абелева.*

Теорема 2.5. *Всякая подгруппа циклической группы является циклической.*

Итак, в любой группе много циклических подгрупп: каждый элемент порождает свою циклическую подгруппу. Тем не менее, следует заметить, что чаще группы циклическими не являются. Например, все некоммутативные

группы не могут быть циклическими. Циклическими не являются аддитивные и мультипликативные группы вещественных и комплексных чисел в силу их несчетности. Множество рациональных чисел счетно, то есть равномощно множеству целых чисел. Однако абелева группа (Q, +) в отличие от группы (Z, +) из примера 2.10 также не циклична, т.к. для каждого рационального числа $q = \frac{n}{m} \in Q$ подгруппа $\langle q \rangle = \left\{ 0; \pm\frac{n}{m}; \pm\frac{2n}{m}; \pm\frac{3n}{m}; \ldots \right\}$ не содержит рациональных несократимых дробей $\frac{r}{s}, r \in Z, s \in N$, у которых знаменатель $s > m$, следовательно, $\langle q \rangle \neq (Q, +)$.

Теорема 2.6. *Для каждого простого числа p мультипликативная группа Z / pZ^* содержит p – 1 элементов и является циклической.*

Проблема нерешенная [16]: конечно или бесконечно множество простых чисел p, для которых $Z / pZ^* = \langle \overline{2} \rangle$, т.е. мультипликативная группа Z / pZ^* совпадает с циклической подгруппой, порожденной классом вычетов $\overline{2}$?

2.4. Смежные классы по подгруппе

Определение 2.11. *Пусть H – собственная подгруппа группы* (G, ·). *Пусть $a \in G$. Через aH обозначим множество элементов $\{ah \mid h \in H\}$ и назовем его левым смежным классом группы G по подгруппе H.*

Если существует $b \in G, b \notin H \cup aH$, можно построить новый левый смежный класс bH и так далее. Аналогично строят правые смежные классы. Если каждый левый смежный класс совпадает с правым: $aH = Ha$, то тогда смежные классы называют двусторонними. Такими являются смежные классы в любой абелевой группе G. Смежные классы обладают рядом важных свойств, которые отражает

Теорема 2.7. *Пусть H – собственная подгруппа группы G. Тогда:*

1) *каждый элемент $g \in G$ принадлежит какому-нибудь левому смежному классу по подгруппе H;*
2) *два элемента $a, b \in G$ принадлежат одному левому смежному классу тогда и только тогда, когда $a^{-1} \cdot b \in H$;*
3) *любые два левых смежных класса либо не пересекаются, либо совпадают;*
4) *для всякого $a \in G$ мощности множеств aH и H совпадают;*
5) *G есть объединение попарно непересекающихся левых (правых) смежных классов по подгруппе H.*

Пример 2.14. Пусть $G = M_{1\times 4}(Z / 2Z)$ – множество всевозможных строк-матриц с четырьмя координатами из $Z / 2Z$. Это группа по сложению. Обычно ее обозначают через V_4. Легко проверить, что множество

$H = \left\{ \underbrace{(0\ \ 0\ \ 0\ \ 0)}_{\bar{0}}, \underbrace{(1\ \ 0\ \ 1\ \ 1)}_{e_1}, \underbrace{(0\ \ 1\ \ 0\ \ 1)}_{e_2}, \underbrace{(1\ \ 1\ \ 1\ \ 0)}_{e_1+e_2} \right\}$ образует подгруппу в группе V_4. Очевидно, $|G| = 24 = 16, |H| = 4$. Согласно теореме 2.7 группа G представляет собой объединение четырех смежных классов по подгруппе H. Эти классы представлены в таблице.

Смежные классы группы G по подгруппе H

№	Класс $a + H$	$\bar{a} + \bar{0}$	$\bar{a} + \overline{e_1}$	$\bar{a} + \overline{e_2}$	$\bar{a} + (\overline{e_1} + \overline{e_2})$
1	$\bar{0} + H = H$	(0000)	(1011)	(0101)	(1110)
2	$(1000) + H$	(1000)	(0011)	(1101)	(0110)
3	$(0100) + H$	(0100)	(1111)	(1001)	(1010)
4	$(0010) + H$	(0010)	(1001)	(0111)	(1100)

Лемма 2.3. *Пусть H – собственная подгруппа группы G. Мощности множеств всех левых и соответственно правых смежных классов группы G по подгруппе H равны.*

Доказательство. Построим соответствие между названными множествами по правилу $gH \leftrightarrow Hg$. Очевидно, такое соответствие является взаимно однозначным, что и доказывает лемму.

Доказанное утверждение позволяет ввести следующее

Определение 2.12. *Индексом подгруппы H в группе G называется мощность множества всех смежных классов группы G по данной подгруппе и обозначается через $|G : H|$.*

Пример 2.15. Индекс подгруппы $(nZ, +)$ в группе $(Z, +)$ равен n. Действительно, в данном случае множество всех смежных классов есть множество $\{nZ.1 + nZ, 2 + nZ, \ldots, (n-1) + nZ\}$.

Замечание. Таблицы смежных классов играют важную роль в теории и практике помехоустойчивого кодирования. Простейший метод коррекции ошибок базируется на основе таблиц смежных классов, аналогичных приведенной выше. В современных цифровых каналах связи принято информацию передавать в виде двоичных блоков с определенной фиксированной длиной n, то есть n-мерных векторов с координатами из $Z/2Z$. Они получаются разбиением исходной информации, уже преобразованной в двоичный текст, на блоки по k двоичных символов, $k < n$. К каждому k-мерному блоку присоединяется специальным образом $n - k$ проверочных разрядов. В результате предназначенные для передачи слова принадлежат некоторому k-мерному подпространству H пространства V_n всех n-мерных векторов. С точки зрения теории групп H – подгруппа аддитивной группы V_n. Ее называют группой кодовых слов. В процессе передачи по каналу связи конкретного кодового слова $\bar{h}$ может наложиться «шум» – некоторый n-мерный двоичный вектор $\bar{e} \in V_n$. Тогда принятое по каналу связи слово-сообщение $\bar{x} = \bar{h} + \bar{l}$ является одним из элементов таблицы смежных классов группы V_n, образующая смежного класса и есть наложив-

шийся в процессе передачи на $\bar{h}$ вектор ошибок $\bar{e}$. Если мы имеем в своем распоряжении таблицу смежных классов группы V_n по подгруппе *H*, то по полученному $\bar{x}$ мы легко определяем вектор ошибок $\bar{e}$ (первый элемент строки, содержащий $\bar{x}$) и истинное сообщение $\bar{h}$ (первый элемент столбца, в который попадает $\bar{x}$).

2.5. Теорема Лагранжа

Теорема 2.8 (Лагранжа). *Порядок конечной группы делится на порядок любой ее подгруппы.*

Доказательство. Пусть *H* – подгруппа конечной группы *G*. Пусть $|G| = n, |H| = m$. Согласно теореме 2.7 группа *G* есть объединение непересекающихся смежных классов (левых или правых) по подгруппе *H*, каждый мощностью *m*. Пусть имеется всего *k* различных классов. Тогда $n = km$. Следовательно, $|G|$ делится на $|H|$, что и требовалось доказать.

Следствие 1. *В конечной группе индекс подгруппы равен частному от деления порядка группы на порядок подгруппы.*

Следствие 2. *Любая группа простого порядка является циклической и не содержит собственных подгрупп.*

Пример 2.16. Всякая группа, порядок которой равен одному из следующих чисел: 1949, 1951, 1973, 1979, 1987, 1993, 1997, 1999, 2003, 2011, 2017 является циклической.

Следствие 3. *Если G – конечная группа из n элементов, то для каждого* $a \in G\ a^n = e$. *Другими словами, в конечной группе порядок любого ее элемента делит порядок самой группы.*

В связи с теоремой Лагранжа возникает следующий вопрос: существует ли для всякого делителя *m* порядка *n* конечной группы *G* подгруппа *H* порядка *m*?

Вообще, ответ на данный вопрос отрицательный. Тем не менее, для циклических групп ответ положителен.

Теорема 2.9. *В циклической группе G для каждого делителя m порядка* $|G|$ *найдется подгруппа из m элементов.*

2.6. Нормальные подгруппы и фактор-группы

Определение 2.13. *Собственная подгруппа H группы G называется нормальной, если для всякого* $a \in G\ a \cdot H = H \cdot a = e$, *то есть каждый левый смежный класс по подгруппе H совпадает с правым смежным классом. В этом случае пишут* $H \Delta G$.

Ясно, что у абелевых групп все подгруппы нормальные. Очевидно, всякая подгруппа индекса 2 является нормальной.

Теорема 2.10. $H \Delta G$ *тогда и только тогда, когда для каждого* $a \in G\ aHa^{-1} = H$.

Пример 2.17. Подгруппа $SL_n(R)$ – множество квадратных матриц поряд-

ка $n>1$ с определителем, равным 1, является нормальной подгруппой группы $GL_n(R)$ – множества квадратных матриц порядка $n>1$ с вещественными коэффициентами и ненулевым определителем, поскольку для всякой матрицы $B \in SL_n(R)$ и произвольной матрицы $A \in GL_n(R)$

$$A \in GL_n(R)\ \det\left(ABA^{-1}\right) = \det(A)\cdot\det(B)\cdot\det(A)^{-1} = \det(B) = 1.$$

Определение 2.14. *Пусть* $(G, \cdot)$ *– группа и H – ее подгруппа. Факторможеством (левым) группы G по подгруппе H называется множество всех левых смежных классов* $\{H, aH, bH, \ldots\}$ *и обозначается через G/H.*

Пусть H – нормальная подгруппа. Определим умножение на факторможестве G/H по следующему правилу: $aH \cdot bH = (ab)H$. Операция полностью определяется умножением элементов группы G, поэтому ее называют индуцированной операцией умножения на фактор-множестве.

Теорема 2.11. *Относительно индуцированной операции факторможество G/H по нормальной подгруппе H является группой.*

Пример 2.18. Группа $(Z, +)$ содержит для всякого натурального $n>1$ нормальную подгруппу $(nZ, +)$. Следовательно, определена фактор-группа G/H. Это не что иное, как рассмотренная ранее $(Z/nZ, \oplus)$, – группа классов вычетов по модулю n относительно операции сложения классов.

2.7. Симметрическая группа

Пусть Ω – конечное множество из n элементов. Поскольку конкретная природа его элементов несущественна, удобно считать, что $\Omega = \{1,2,\ldots,n\}$. Всякое биективное, то есть взаимно однозначное отображение Ω в себя называется подстановкой на Ω. Подстановку $f: i \to f(i), i = 1,2,\ldots,n$ удобно изображать в развернутой и наглядной форме в виде двустрочной таблицы:

$$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix}.$$

В этой таблице каждый i-й столбец четко указывает, в какой элемент $f(i)$ преобразуется элемент $i, 1 \le i \le n$.

Подстановки перемножаются в соответствии с общим правилом композиции отображений: $(gf)(i) = g(f(i))$.

Пример 2.19. Пусть $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$. Найдем fg. $g: 1 \to 2$, $f: 2 \to 5$; $g: 2 \to 4$, $f: 4 \to 1$; $g: 3 \to 5$, $f: 5 \to 4$; $g: 3 \to 5$, $f: 5 \to 4$; $g: 4 \to 1$, $f: 1 \to 3$; $g: 5 \to 3$, $f: 3 \to 2$. Получаем: $fg = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{pmatrix}$. Найдем gf. Аналогично предыдущему

$$gf = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix}.$$

Как видим $gf \neq fg$, то есть композиция подстановок не обладает свойст-

вом коммутативности.

Очевидно, тождественная подстановка $e=\begin{pmatrix}1 & 2 & \dots & n\\ 1 & 2 & \dots & n\end{pmatrix}$ играет роль единицы относительно композиции подстановок. Как известно, композиция отображений является ассоциативной операцией, поэтому и композиция подстановок ассоциативна. Каждая подстановка – обратимая операция. Чтобы найти для подстановки f обратную подстановку f^{-1}, достаточно в таблице $\begin{pmatrix}1 & 2 & \dots & n\\ f(1) & f(2) & \dots & f(n)\end{pmatrix}$ переставить строки местами, а затем столбцы упорядочить по возрастанию элементов первой строки.

Пример 2.20. Для подстановки f из предыдущего примера 2.19 найти f^{-1}.

$$f=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 3 & 5 & 2 & 1 & 4\end{pmatrix},\ f^{-1}=\begin{pmatrix}3 & 5 & 2 & 1 & 4\\ 1 & 2 & 3 & 4 & 5\end{pmatrix}=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 4 & 3 & 1 & 5 & 2\end{pmatrix}.$$

Проверим правильность результата, для чего найдем композиции:

$$f^{-1}f=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 4 & 3 & 1 & 5 & 2\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 3 & 5 & 2 & 1 & 4\end{pmatrix}=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 2 & 3 & 4 & 5\end{pmatrix}=e,$$

$$f\cdot f^{-1}=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 3 & 5 & 2 & 1 & 4\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 4 & 3 & 1 & 5 & 2\end{pmatrix}=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 2 & 3 & 4 & 5\end{pmatrix}=e.$$

Таким образом, подстановки на Ω образуют группу с операцией композиции подстановок.

Определение 2.15. *Симметрической группой степени n называют группу подстановок на n элементах относительно операции умножения подстановок (композиции отображений) и обозначают через* S_n.

Теорема 2.12. *Порядок группы* S_n *равен n!*

Доказательство методом математической индукции. При $n=2$ на множестве $\Omega=\{1,2\}$ существует в точности $2!=2$ различных подстановок – это тождественная подстановка *e* и подстановка *f*, такая, что $f(1)=2,\ f(2)=1$. Предположим по индукции, что $|S_{n-1}|=(n-1)!$ Перечислим все возможные подстановки на *n*-элементном множестве. В качестве $f(1)$ можно взять любой из элементов множества $\Omega=\{1,2,\dots,n\}$. На долю остальных значений остается по предположению индукции $(n-1)!$ возможностей. Таким образом, $|S_{n-1}|=n(n-1)=n!$, что и требовалось доказать.

Пример 2.21. В силу теоремы 2.12 $|S_2|=2;|S_3|=6;|S_4|=24;|S_5|=120$.

Разложим подстановки из S_n в произведение более простых подстановок. Идею разложения поясним на примере подстановок *f* и *g*, указанных на рис. 1:

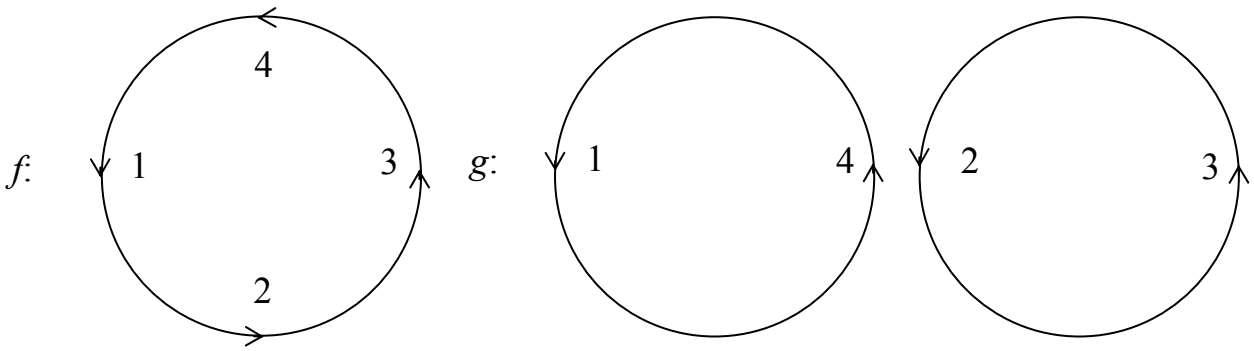

Рисунок 1

Подстановка f кратко записывается в виде $f=(1,2,3,4)$ или, если это не вызывает разночтений в виде $f=(1234)$ и носит название цикла длиной 4, а подстановка g записывается в виде $g=(14)(23)$ произведения двух независимых (непересекающихся) циклов (14) и (23) длиной два.

Например, $f=\begin{pmatrix}1&2&3&4&5&6&7&8\\3&1&2&7&6&5&4&8\end{pmatrix}$ можно записать в виде произведения циклов $(132)(47)(56)(8)=(132)(47)(56)$, так как естественно в произведении $f=f_1f_2\ldots f_p$ опускать сомножители, соответствующие Ω_i из одного элемента, потому что $f_i=e$ – тождественная подстановка на Ω.

Теорема 2.13. *Каждая подстановка $f\in S_n$, $f\neq l$, является произведением независимых циклов длиной $l\geq 2$. Это разложение в произведение определено однозначно с точностью до порядка следования циклов.*

Определение 2.16. *Цикл длиной 2 называется транспозицией.*

Теорема 2.14. *Каждая подстановка $f\in S_n$, $f\neq l$ раскладывается в произведение транспозиций.*

Доказательство. Согласно теореме 2.13 f раскладывается в произведение независимых циклов. Каждый цикл раскладывается в произведение независимых транспозиций. Примером такого разложения является следующее, легко проверяемое равенство: $(i_1i_2\ldots i_k)=(i_1i_k)\cdot(i_1i_{k-1})\cdot\ldots\cdot(i_1i_3)\cdot(i_1i_2)$.

Пример 2.22. Разложить в произведение циклов и транспозиций подстановку

$$g=\begin{pmatrix}1&2&3&4&5&6&7&8\\3&1&4&2&6&5&8&7\end{pmatrix}.$$

Решение. $g=(1342)(56)(78)=(12)(14)(13)(56)(78)$.

Разложение подстановки в произведение транспозиций неоднозначно. Тем не менее, справедлива

Теорема 2.15. *Любые два разложения данной подстановки в произведение транспозиций содержат либо четное число сомножителей, либо нечетное.*

Определение 2.17. *Подстановка f называется четной (нечетной), если ее разложение в произведение транспозиций содержит четное (нечетное) ко-*

личество сомножителей.

Пример 2.23. «Игра в пятнадцать»: на квадратной доске, разделенной на 16 полей, размещены 15 фишек, пронумерованных от 1 до 15 и занимающих целиком соответствующее поле. Двигая фишки по горизонтали и вертикали с использованием свободного поля, требуется привести доску в состояние (1) (рис. 2).

i_1	i_2	i_3	i_4
i_5	i_6	i_7	i_8
i_9	i_{10}	i_{11}	i_{12}
i_{13}	i_{14}	i_{15}	

$\rightarrow$

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Рисунок 2

Можно показать, что задача разрешима тогда и только тогда, когда подстановка $f = \begin{pmatrix} 1 & 2 & \dots & 15 \\ i_1 & i_2 & \dots & i_{15} \end{pmatrix}$ четная. Возможно ли привести положение на доске (рис. 3) в состояние (1)?

2	1	3	4
5	6	7	8
9	10	11	12
13	14	15	

Рисунок 3

Здесь $f = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & 15 \\ 2 & 1 & 3 & 4 & \dots & 15 \end{pmatrix} = (12)(3)(4)\dots(15) = (12)$, подстановка нечетная. Следовательно, задача, за которую почти 130 лет тому назад предлагали большой денежный приз, не имеет решения.

2.8. Криптосистема RSA

Понятие группы считается основополагающим в математике XX века. Группы широко применяются в физике (от кристаллографии до теории элементарных частиц), химии, биологии, теории информации. Новейшие методы защиты информации от несанкционированного доступа называют групповыми, так как они базируются на понятии группы. Ярким примером является криптосистема RSA, предложенная в 1977 г. американскими исследователями Ривестом, Шамиром и Адлеманом (Riverst R.L., Shamir A., Adleman L.). Суть ее в следующем.

Находятся два больших простых числа (60-70 десятичных знаков) p и g. Вычисляется их произведение $n = p \cdot g$. Тогда (свойства 3, 1 функции Эйлера) $\varphi(n) = \varphi(p \cdot g) = \varphi(p) \cdot \varphi(p) = (p-1) \cdot (g-1)$. Фиксируется натуральное число e, $0 < e < n$, $НОД(e, \varphi(n)) = 1$. Пара (e, n) называется открытым ключом. Передаваемая информация переводится в цифровую форму (в первоисточнике буквы латинского алфавита заменяются двузначными числами: $"a" = 01, "b" = 02$ и так

далее, пробел = 00), шифруется в виде числа c – сообщения, $0 < c < n$, $НОД(c, n) = 1$. Тогда c есть обратимый элемент кольца Z/nZ, то есть элемент абелевой группы (Z/nZ)* порядка $\varphi(n)$. Сообщение шифруется и передается числом $m \equiv c^e \pmod n$. Таким образом, m есть e-я степень числа c в кольце Z/nZ.

Адресат получает сообщение m. Он, как и все, знает величины n и e. Он также должен знать секретный ключ – такое натуральное число $d < n$, что $e \cdot d \equiv 1(\mathrm{mod}\,\varphi(n))$. По определению это означает, что $e \cdot d = 1 + \varphi(n) \cdot q$ для некоторого целого q. Тогда $\overline{m}^d = \overline{c}^{ed} = \overline{c}^{1+\varphi(n)\cdot r} = \left(\overline{c}^{\varphi(n)}\right)^r \cdot \overline{c} = 1 \cdot \overline{c} = \overline{c}$. Чтобы расшифровать m адресат должен возвести m в d-ю степень по модулю n. Это простая задача.

Перехватчик, чтобы расшифровать сообщение m, должен разложить n на множители: $n = pq$. Тогда вычисляется $\varphi(n)$ и d легко находится по открытому ключу e. Именно разложение ключа n на множители и составляет основную сложность предлагаемой криптосистемы. Как было отмечено в первом разделе, разложение натурального числа на множители является, по всей видимости, экспоненциальной относительно n задачей, эквивалентной перебору всех возможных кандидатов на делители.

Чтобы продемонстрировать стойкость своей криптосистемы, изобретатели зашифровали свое сообщение, используя в качестве n – 129-значное число и в качестве e – 4-значное число. Их сообщение m было 128-значным числом. Всемирно известный американский специалист по головоломкам М. Гарднер опубликовал этот криптотекст в журнале «Scientific American» в августе 1977 г., предложив 1000 долларов тому, кто его расшифрует. Текст был расшифрован лишь в апреле 1994 г. 129-значное число n было разложено на 64- и 65-значные множители p и q. Непосредственная факторизация числа n заняла полтора года вычислений. После этого расшифровка сообщения не составила труда.

2.9. Кольца. Подкольца и идеалы колец

Определение 2.18. *Кольцом называется непустое множество K с двумя бинарными алгебраическими операциями сложения* (+) *и умножения (·); относительно операции сложения K является абелевой группой, а умножение и сложение связаны законами дистрибутивности:*

$(a + b) \cdot c = a \cdot c + b \cdot c;\ a(b + c) = ab + ac$ *для произвольных* $a, b, c \in K$.

Пример 2.24. (Z, +, ·) – кольцо целых чисел.

Пример 2.25. (Z/nZ, +, ·) – кольцо классов вычетов по модулю $n > 1$.

Пример 2.26. Множество всех квадратных матриц данного порядка n с рациональными, вещественными или же комплексными коэффициентами относительно операций матричного сложения и умножения. Общепринятые обозначения этих колец: $M_n(Q), M_n(R), M_n(C)$ соответственно.

Многообразие колец чрезвычайно широко. По числу элементов кольца делятся на конечные (пример 2.25) и бесконечные (примеры 2.24, 2.26). Основная классификация колец ведется по свойствам умножения.

Определение 2.19. *Кольцо K называется ассоциативным кольцом, если*

определенная на нем операция умножения обладает свойством: $(ab)c = a(bc)$ *для произвольных* $a, b, c \in K$.

Кольцо K называется кольцом с единицей, если оно ассоциативно и имеет нейтральный элемент относительно операции умножения.

Кольцо K называется коммутативным, если $ba = ab$ *для произвольных* $a, b \in K$.

Теорема 2.16. *Пусть K – ассоциативное кольцо с единицей. Множество K* обратимых относительно умножения элементов кольца K есть группа (ее называют мультипликативной группой кольца K).*

Пример 2.27. Легко видеть, что в кольце целых чисел обратимы относительно умножения только два числа: 1 и –1. Следовательно, $Z^* = \{1, -1\}$.

Пример 2.28. $M_n(R)^* = GL_n(R)$.

Пример 2.29. Мультипликативная группа $(Z/nZ)^*$ кольца классов вычетов Z/nZ по модулю n состоит из $\varphi(n)$ классов, порожденных целыми числами, взаимно простыми с модулем.

Определение 2.20. *Если в кольце K с единицей мультипликативная группа* $K^* = K \setminus \{0\}$*, то кольцо K называют телом или алгеброй с делением. Коммутативное тело называют полем.*

Пример 2.30. Следующие кольца являются полями:

а) Q – кольцо рациональных чисел;

б) R – кольцо вещественных чисел;

в) C – кольцо комплексных чисел;

г) Z/pZ – кольцо классов вычетов по простому модулю p.

Определение 2.21. *Подкольцо кольца K – это подгруппа аддитивной группы* $(K, +)$*, в свою очередь являющаяся кольцом, то есть замкнутая относительно операции умножения в кольце K.*

Пример 2.31. $(nZ, +, \cdot)$ – подкольцо кольца Z целых чисел; Z – подкольцо кольца Q рациональных чисел; Q – подкольцо кольца R вещественных чисел. Первое из них – это кольцо без единицы, хотя само кольцо Z с единицей.

Подкольца, в общем случае, практически не наследуют свойства колец. Поэтому в теории колец наибольшее значение имеют подкольца специального вида – идеалы.

Определение 2.22. *Подкольцо J кольца K называется левым идеалом кольца K, если для любого* $k \in K$ *и для каждого* $j \in J$ *произведение* $jk \in J$*, то есть* $Jk \subseteq J$*. Если же* $kJ \subseteq J$ *для всех элементов* $k \in K$*, то J называют правым идеалом. Двусторонний идеал – идеал, являющийся одновременно и левым и правым идеалом.*

Ясно, что в коммутативном кольце все идеалы двусторонние.

Пример 2.32. $mZ = \{mg \mid g \in Z\}$ – двусторонний идеал кольца целых чисел Z для всякого натурального m. Очевидно, $mZ \neq Z$, если $m > 1$. Ясно, что $2z > 4z > 8z > 16z > \ldots$; $2z > 6z > 12z > \ldots$.

Пример 2.33. В кольце Z/nZ с составным модулем $n = pq$, $p > 1, q > 1$, легко видеть, что множество классов вычетов $\{\overline{p}, \overline{2p}, \ldots, \overline{(q\text{-}1)p}, \overline{0}\}$ замкнуто от-

носительно операций сложения и умножения классов вычетов и, следовательно, образует подкольцо. Обозначим его через $J_{\overline{p}}$. Легко видеть, что $J_{\overline{p}}$ – идеал. Аналогично идеалом является множество $J_{\overline{q}} = \{\overline{q}, \overline{2q}, \ldots, \overline{(p-1)q}, \overline{0}\}$.

Пример 2.34. В любом кольце K множество $\{0\}$ и K формально также являются идеалами кольца K. Их называют несобственными, или тривиальными, в отличие от остальных – собственных идеалов.

Теорема 2.17. ***1.*** *Пересечение идеалов данного кольца K есть идеал этого же кольца.*

2. Если J_1, J_2 – левые (правые) идеалы кольца K, то их сумма, то есть множество всех сумм $\{j_1 + j_2 \mid j_1 \in J_1;\ j_2 \in J_2\}$, есть левый (правый) идеал кольца K.

3. Произведение $J_1 J_2 = \{j_1 \cdot j_2 \mid j_1 \in J_1;\ j_2 \in J_2\}$ левых (правых) идеалов J_1, J_2 кольца K есть левый (правый) идеал этого же кольца.

4. Для каждого элемента a кольца K множество $aK = \{ak \mid k \in K\}$ есть левый идеал кольца K.

5. Если в кольце K с единицей элемент $a \in K^*$, то $\langle a \rangle = K$; если же $a \notin K^*$, то $\langle a \rangle$ – собственный идеал кольца K.

6. Если K – коммутативное кольцо и $a = bc$ для необратимых элементов $a, b, c \in K$, то $\langle a \rangle \subset \langle c \rangle, \langle a \rangle \subset \langle b \rangle$.

Доказательство состоит в прямой проверке всех аксиом идеалов.

Определение 2.23. *Левым главным идеалом $\langle a \rangle$ кольца K, порожденным элементом $a \in K$, называется идеал из 4-го пункта теоремы 2.17, то есть подкольцо кольца K, состоящее из всех элементов $ak, k \in K$. Правый главный идеал $\langle a \rangle$ состоит из всех элементов $ka, k \in K$.*

Теорема 2.18. ***В*** *кольце целых чисел Z – всякий идеал J – главный.*

На множестве идеалов каждого кольца существует отношение частичного порядка по включению их друг в друга как множеств. Особую роль играют максимальные идеалы.

Определение 2.24. *Идеал M (левый, правый, двусторонний) кольца K называется максимальным, если в K не существует собственного идеала J с условием $M \in J$.*

Теорема 2.19. ***В*** *кольце целых чисел идеал J максимален тогда и только тогда, когда существует простое число p, такое, что $J = \langle p \rangle$.*

2.10. Делимость в кольце многочленов

Пусть P – поле, то есть произвольное коммутативное кольцо с единицей, у которого все элементы, отличные от нуля, обратимы, иными словами, $P^* = P \setminus \{0\}$. Например, $P = Q, R, C, Z / pZ$.

Пусть $P[x]$ – кольцо многочленов с коэффициентами из P с обычными операциями сложения и умножения многочленов. По своим свойствам многочлены близки к целым числам. Например, как и для целых чисел имеет место

Теорема 2.20 (о делении с остатком). ***Для любых двух многочленов*** $f(x)$ ***и*** $g(x)\neq 0$ ***из кольца*** $P[x]$ ***существуют единственные многочлены*** $q(x)$ ***и*** $r(x)$***, такие, что*** $f(x)=g(x)q(x)+r(x)$***, причем*** $r(x)=0$ ***или степень*** $r(x)$ ***меньше степени*** $g(x)$**.**

Определение 2.25. *В условиях теоремы 2.20 многочлен* $q(x)$ *называется частным, а многочлен* $r(x)$ *– остатком от деления* $f(x)$ *на* $g(x)$*. Если* $r(x)=0$*, то говорят, что* $f(x)$ *делится на* $g(x)$*, а* $g(x)$ *и* $q(x)$ *называют делителями или множителями многочлена* $f(x)$*.*

Если в равенстве $f(x)=g(x)\cdot q(x)$ степени сомножителей не меньше 1, то $q(x)$ и $g(x)$ называют нетривиальными делителями многочлена $f(x)$.

Очевидно, каждый ненулевой элемент поля *P* является делителем любого многочлена из кольца $P[x]$. Поэтому элементы полей называют тривиальными делителями многочленов.

Теорема 2.21. ***Обратимыми многочленами в кольце многочленов*** $P[x]$ ***являются многочлены нулевой степени, отличные от нуля, и только они, то есть*** $P[x]^{*}=P^{*}$**.**

Определение 2.26. *Наибольшим общим делителем многочленов* $f_1(x), f_2(x), \ldots, f_5(x)$ *называется их общий делитель со старшим коэффициентом* 1*, который делится на любой другой общий делитель. Его обозначают* $НОД(f_1(x), f_2(x), \ldots, f_s(x))$*.*

Алгоритм Евклида нахождения *НОД*, рассмотренный ранее в разделе 1 для целых чисел, справедлив и для многочленов.

Теорема 2.22. *Наибольший общий делитель многочленов* $f(x)$ *и* $g(x)$ *из кольца* $P[x]$ *(с точностью до множителей из поля P) совпадает с последним отличным от нуля остатком* $r_n(x)$ *следующей цепочки равенств:*

$$\begin{cases} f(x)=g(x)q_1(x)+r_1(x); \\ g(x)=r_1(x)q_2(x)+r_2(x); \\ r_1(x)=r_2(x)q_3(x)+r_3(x); \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ r_{n-2}(x)=r_{n-1}(x)q_n(x)+r_n(x); \\ r_{n-}(x)=r_n(x)q_{n+1}(x). \end{cases}$$

Пример 2.35. Найти при помощи алгоритма Евклида наибольший общий делитель многочленов $f(x)=2x^4+5x^3-8x^2-17x-6$ и $g(x)=x^3+4x^2-x-4$ в кольце $Q[x]$.

Решение. Последовательным делением «уголком» получаем следующую цепочку равенств алгоритма Евклида:

$f(x)=g(x)\cdot q_1(x)+r_1(x)$, где $q_1(x)=2x-3, \quad r_1(x)=6x^2-12x-18$,

$g(x)=r_1(x)q_2(x)+r_2(x)$, где $q_2(x)=\frac{1}{6}x+1, \quad r_2(x)=14x+14$,

$r_1(x) = r_2(x)q_3(x) + r_3(x)$, где $q_3(x) = \frac{3}{7}(x-3)$, то есть $r_1(x) = 6(x+1)(x-3)$.

Согласно теореме 2.22 наибольший общий делитель по алгоритму Евклида получается с точностью до константы. Таким образом, $НОД(f(x), g(x)) = x+1$.

Определение 2.27. *Многочлены $f(x)$ и $g(x)$ называют взаимно простыми, если их наибольший общий делитель равен 1.*

Обратной прогонкой алгоритма Евклида (аналогично целым числам) получается критерий взаимной простоты двух многочленов.

Теорема 2.23. *Многочлены $f(x)$ и $g(x)$ являются взаимно простыми тогда и только тогда, когда найдутся такие многочлены $u(x)$, $v(x)$, для которых выполняется следующее равенство (соотношение Безу для многочленов): $f(x)u(x) + g(x)v(x) = 1$.*

С помощью этого критерия получается ряд следствий, имеющих независимое значение. Приведем их в виде отдельных утверждений.

Утверждение 2.1. *Если многочлен $f(x)$ взаимно прост с каждым из многочленов $\varphi(x)$ и $\psi(x)$, то он взаимно прост и с их произведением.*

Утверждение 2.2. *Если произведение многочленов $f(x)$ и $g(x)$ делится на многочлен $\varphi(x)$, но $НОД(f(x), \varphi(x)) = 1$, то $g(x)$ делится на $\varphi(x)$.*

Утверждение 2.3. *Если многочлен $f(x)$ делится на каждый из попарно взаимно простых многочленов $\varphi_1(x), \varphi_2(x), \ldots, \varphi_m(x)$, то $f(x)$ делится и на их произведение $\varphi_1(x) \cdot \varphi_2(x) \cdot \ldots \cdot \varphi_m(x)$.*

Определение 2.28. *Многочлен $f(x) \in P[x]$ степени $n \geq 1$ называется неприводимым в кольце $P[x]$, если в любом его представлении в виде произведения $f(x) = g(x)q(x)$ сомножителей $g(x), q(x) \in P[x]$ один из этих сомножителей является константой, то есть элементом поля P.*

Структура неприводимых многочленов существенно зависит от поля P. Если $P = C$ – поле комплексных чисел, то неприводимыми многочленами в $C[x]$ являются только многочлены первой степени согласно основной теореме алгебры. Отсюда следует, что в кольце $R[x]$ неприводимыми являются лишь многочлены первой степени, а также второй степени с отрицательным дискриминантом. Что касается кольца $Q[x]$, то здесь для каждого натурального $n \geq 1$ существуют (причем бесконечно много) неприводимые многочлены степени n. К примеру, таковыми являются многочлены $x^n \pm p$, где p – простое число согласно следующему критерию.

Теорема 2.24 (критерий Эйзенштейна). *Пусть $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ – многочлен степени $n > 1$ с целыми коэффициентами и p – такое простое число, что $a_i \equiv 0 (\mathrm{mod}\, p)$ для всех $i < n$, но a_n не делится на p, и a_0 не делится на p^2. Тогда $f(x)$ – неприводимый в кольце $Q[x]$ многочлен.*

В кольце $(Z/pZ)[x]$ также существуют неприводимые многочлены любой степени $n \geq 1$. Только в отличие от $Q[x]$ здесь произвольных многочленов степени *n* имеется лишь конечное множество (в количестве p^{n+1}), тем более число неприводимых многочленов данной степени всегда конечно. Обычно неприводимость многочлена над конечным полем определяется процедурой просеивания, напоминающий решето Эратосфена для целых чисел – последовательным делением на неприводимые (или все) меньшей степени от 1 до $[n/2]$. В качестве примера приведем список всех неприводимых многочленов в кольце $(Z/2Z)[x]$ степени, меньшей шести.

1) x;
2) x+1;
3) x^3+x+1;
4) x^2+x+1;
5) x^3+x^2+1;
6) x^4+x^3+x^2+1;x
7) x^4+x+1;
8) x^4+x^3+1;
9) x^5+x^2+1;
10) x^5+x^3+1;
11) x^5+x^3+x^2+x+1;
12) x^5+x^4+x^2+x+1;
13) x^5+x^4+x^3+x+1;
14) x^5+x^4+x^3+x^2+x+1;

Неприводимые многочлены играют роль простых чисел кольца целых чисел. Следующая теорема аналогична теореме 1.5.1.

Теорема 2.25. *Всякий многочлен* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in P[x]$ *степени* $n \geq 1$ *представим в виде произведения* $f(x) = a_n p_1(x) p_2(x) \ldots p_s(x)$, *где* $p_i(x)$ *– неприводимые многочлены со старшим коэффициентом, равным 1. Такое представление единственно с точностью до порядка сомножителей.*

Процедура конкретной факторизации многочлена в произведение неприводимых многочленов достаточно трудоемка, зависит существенным образом от поля коэффициентов, имеет много методик и подходов. Над полем комплексных чисел она эквивалентна, в силу основной теоремы алгебры и теоремы Безу, решению алгебраических уравнений. Над другими полями решение алгебраических уравнений включается лишь как один из этапов факторизации. Над конечными полями факторизовать многочлены можно аналогом Эратосфена.

2.11. Основы теории полей

Поля выделяются из общего многообразия коммутативных колец наличием максимально возможной мультипликативной группы – в нее входят все не-

нулевые элементы, отсутствием делителей нуля, отсутствием собственных идеалов. Неотъемлемым атрибутом, важнейшим из свойств каждого поля является его характеристика.

Определение 2.29. *Если в поле P существует такое натуральное n, что равна нулю сумма n единиц (n раз складывается с самим собой 1 – нейтральный элемент относительно умножения):* $1+1+\ldots+1=0$, *то наименьшее n с таким свойством называется характеристикой поля P и обозначается через* $charP$. *Если в поле P любая конечная сумма единиц отлична от нуля, то говорят, что характеристика поля P равна* 0.

Теорема 2.26. *Если характеристика поля отлична от нуля, то она является числом простым.*

Пример 2.36. В поле $P = Z / pZ$, p – простое число, характеристика равна p. В самом деле, Z / pZ является аддитивной группой из p элементов и, следовательно, циклической группой порядка p, порожденной любым ненулевым элементом, в частности, единицей – нейтральным элементом относительно умножения. Согласно теореме 2.3 о структуре циклических групп $Z / pZ = \left\{\overline{1}, \overline{1}+1=\overline{2}, \ldots, \overline{1}+\overline{1}+\ldots+\overline{1}=\overline{p-1}, \overline{1}+\overline{1}+\ldots+\overline{1}=\overline{0}\right\}$. Это и означает, что $char\left(Z / pZ\right) = P$.

Пример 2.37. Поля Q,R,C имеют характеристику 0.

Определение 2.30. *Поле P называется подполем поля* P', *если все его элементы принадлежат полю* P'.

Теорема 2.27. *Если подполе поля P имеет характеристику p, то и поле P имеет ту же характеристику. Все подполя поля P имеют ту же характеристику.*

Доказательство следует из единственности нейтрального элемента в группе и, следовательно, из единственности единицы в любом поле.

Для нас привычны поля характеристики 0. С этой точки зрения арифметика полей положительной характеристики весьма необычна.

Теорема 2.28. *Пусть P – произвольное поле положительной характеристики p. Пусть n – произвольное число и r – остаток от деления n на p. Тогда для каждого элемента* $a \in P$ *имеет место равенство:* $na = ra$. *В частности, при* $n = pq$ *произведение* $na = pqa = 0$. *Если* $p = 2$, *то при* $n = 2k$ *произведение* $na = 2qa = 0$, *а при* $n = 2k+1$ *произведение* $na = \left(2k+1\right)a = a$.

Доказательство. Произведение $na = a + a + \ldots + a = a\left(1+1+\ldots+1\right)$ – сумма n одинаковых слагаемых, равных a. В силу закона дистрибутивности эта сумма представима в виде произведения a на сумму из n единиц. В силу ассоциативности сложения и определения характеристики сумма каждых p единиц равна нулю. Отсюда и вытекает утверждение теоремы.

Общеизвестна формула бинома Ньютона: $\left(a+b\right)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k$. В полях характеристики p при $n = p^k$ формула бинома Ньютона выглядит совершенно по-другому.

Теорема 2.29. *Пусть* $charP = p > 0$. *Тогда для любых* $a,b \in P$ $(a+b)^p = a^p + b^p$; $(a-b)^p = a^p - b^p$; *а для каждого целого* $k \geq 1$ $(a+b)^{p^k} = a^{p^k} + b^{p^k}$; $(a-b)^{p^k} = a^{p^k} - b^{p^k}$.

Доказательство. Все биномиальные коэффициенты $C_p^k, 1 \leq k < p$, являются целыми числами и вычисляются по формуле: $C_p^k = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\ldots(p-k+1)}{1 \cdot 2 \cdot \ldots \cdot k}$. Числитель данной дроби делится на *p*, ни один из множителей знаменателя не может быть делителем *p* в силу простоты этого числа. Следовательно, C_p^k делится на *p*. Тогда, согласно теореме 2.28, соответствующие слагаемые бинома Ньютона равны нулю, что доказывает первую формулу для бинома Ньютона в характеристике *p*. Остальные формулы доказываются аналогично.

Обычно поле имеет достаточно большой спектр подполей.

Поле рациональных чисел *Q* – подполе поля вещественных чисел *R*, а оно в свою очередь является подполем поля комплексных чисел С. Между *C* и *Q*, между *R* и *Q* существует бесконечно много промежуточных подполей. Для каждого простого числа р многочлен $x^2 - p$ неприводим над *Q*, согласно критерию Эйзенштейна (теорема 2.24); впрочем, можно и непосредственно убедиться, что $\sqrt{p}$ не является рациональным числом. При помощи вычислений можно проверить, что множество $K = \left\{a + b\sqrt{p}; a,b \in Q\right\}$ является полем. Это подполе поля *R*, содержащее *Q* в качестве своего подполя. Аналогично образует поле множество $F = \left\{a + bi; a,b \in Q\right\}$ комплексных рациональных чисел. Оно содержит *Q* и принадлежит полю комплексных чисел *C*.

Определение и основные свойства векторных пространств над полем *R* переносятся на произвольные поля. При этом векторное пространство над конечным полем имеет свои особенности.

Теорема 2.30. *Пусть V – n-мерное линейное пространство над полем* $F(q)$ *из q элементов. Тогда V состоит из* q^n *векторов.*

Определение 2.31. *Если P является подполем поля F, то F называют расширением поля P.*

Определение 2.32. *Расширение F поля P называется конечным (степени n), если размерность векторного пространства F над полем конечна (и равна n). Степень расширения принято обозначать через* $[F : P]$.

Пример 2.38. Поле комплексных чисел является расширением степени два поля вещественных чисел.

Из теоремы 2.30 получаем, что расширение *F* степени *n* конечного поля $F(q)$ из *q* элементов состоит из q^n элементов.

Теорема 2.31 (о башне расширений полей). *Если поле F есть расширение поля P степени n, а поле H – расширение F степени m, то H есть расшире-*

ние P степени $[H:P]=mn$.

Следствие. *Если степень расширения* $[F:P]=q$ *– число простое, то поле F не содержит подполей, промежуточных между F и p.*

Приведем краткие сведения об алгебраических элементах и алгебраических расширениях полей.

Определение 2.33. *Элемент* $\alpha \in f$ *– расширения поля P является алгебраическим над полем P, если существует многочлен* $f(x)\in P[x]$, *корнем которого является α, то есть* $f(\alpha)=0$. *В противном случае α называют трансцендентным полем над P элементом. Поле F называется алгебраическим расширением поля P, если всякий элемент из F является алгебраическим над полем P.*

Общеизвестно, что трансцендентными над Q вещественными числами являются числа π, e. К ним также относятся числа π^e, 0,123456789… – число, содержащее после запятой последовательно записанные числа натурального ряда, многие другие. Известно, что мощность множества вещественных чисел – континуум, а множество всех алгебраических над Q чисел – счетное. Поэтому трансцендентных вещественных чисел существенно больше, чем вещественных алгебраических, чем рациональных чисел.

Теорема 2.32. *Всякое конечное расширение произвольного поля P является алгебраическим над P.*

Следствие 1. *Если расширение F поля P содержит трансцендентные над полем P элементы, то степень этого расширения бесконечна.*

Следствие 2. *Степень расширения* $[R:Q]=+\infty$.

Теорема 2.33. *Для всякого неприводимого многочлена* $f(x)\in P[x]$ *степени* $n>1$ *существует расширение поля P степени n, содержащее корень этого многочлена.*

Пример 2.39. Уравнение $x^3-2=0$ не имеет рациональных корней согласно критерию Эйзенштейна (теорема 2.24). Это уравнение имеет следующие три иррациональных корня: $\sqrt[3]{2};\ \frac{\sqrt[3]{2}\left(-1+i\sqrt{3}\right)}{2};\ \frac{\sqrt[3]{2}\left(-1-i\sqrt{3}\right)}{2}$. Поле $Q\left(\sqrt[3]{2}\right)=\left\{a+b\sqrt[3]{2}+c\sqrt[3]{4};\ a,b,c\in Q\right\}$ содержит только первый из перечисленных корней.

Определение 2.34. *Расширение F поля P называется полем разложения многочлена* $f(x)\in P[x]$, *если оно содержит все корни этого многочлена.*

Такое название мотивировано теоремой Безу о корнях многочленов – при наличии в поле F всех корней многочлена $f(x)$ последний раскладывается в произведение многочленов 1-й степени – двучленов вида $x-\alpha$.

Теорема 2.34. *Для всякого многочлена* $f(x)\in P[x]$ *существует поле* $F\supseteq P$ *– конечное расширение поля P – поле разложения многочлена* $f(x)$.

Далее приведем краткие сведения о конечных полях и их свойствах.

Конечные поля впервые введены в математическую практику в начале XIX века выдающимся французским математиком Эваристом Галуа (1811-1832) – основоположником теории групп. За последнее столетие нет такой об-

ласти математики, развитие которой не было бы в той или иной степени связано с идеями Галуа. Поэтому конечные поля часто называют полями Галуа, а также на письме обозначают через $GF(q)$ – поле Галуа из q элементов. Будем использовать и более краткое обозначение этого поля – $F(q)$. Из предыдущих результатов данного раздела следует

Теорема 2.35. *Любое конечное поле $GF(q)$ элементов имеет конечную характеристику $p > 0$, является конечным расширением поля Z / pZ, содержит $q = p^k$ элементов, при этом k – степень расширения $[GF(q) : Z / pZ]$.*

Из теоремы Лагранжа о конечных группах следует, что все элементы мультипликативной группы $GF(q)^*$ удовлетворяют уравнению $x^{q-1} - 1 = 0$.

Теорема 2.36 (о существовании и единственности конечного поля). *Для каждого простого числа p и для любого $n \geq 1$ натурального существует конечное поле из $q = p^n$ элементов. Это поле единственно с точностью до изоморфизма состоит из корней уравнения $x^q - x = 0$ и только из них.*

Теорема 2.37. *Пусть $F(p^n)$ и $F(p^k)$ – конечные поля, расширения поля $Z / pZ = F(p)$, причем $1 < k < n$. Поле $F(p^k)$ является подполем $F(p^n)$ тогда и только тогда, когда k делит n. Для каждого натурального делителя d числа n существует и единственное подполе $F(p^n)$ из p^d элементов.*

Теорема 2.38. *Мультипликативная группа конечного поля – циклическая.*

Замечание 1. Данная теорема является обобщением теоремы 2.6 о цикличности мультипликативной группы $(Z / pZ)^*$.

Замечание 2. Имеет место следующее обобщение теоремы 2.38: любая конечная подгруппа мультипликативной группы P^* каждого поля P является циклической.

Замечание 3. Мультипликативные группы бесконечных полей не цикличны.

Литература

1. Гусак, А.А. В мире чисел / А.А. Гусак, Г.М. Гусак, Е.А. Гусак. – Минск: Народная асвета, 1987.
2. Липницкий, В.А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа / В.А. Липницкий. – Минск: БГУИР, 2005.
3. Айерхэнд, К. Классическое введение в современную теорию чисел / К. Айерхэнд, М. Роузен. – М.: Мир, 1987.
4. Аршинов, Н.Н. Коды и математика/ Н.Н. Аршинов, Л.Е. Садовский. – М.: Наука, 1983.
5. Бейкер, А. Введение в теорию чисел / А. Бейкер. – Минск: Вышэйшая школа, 1995.
6. Биркгоф, Г. Современная прикладная алгебра / Г. Биркгоф, Т. Барти. – М.:

Мир, 1976.
7. Боро, В. Живые числа. Пять экскурсий / В. Боро, Д. Цагир, Ю Рольфс [и др.] – М.: Мир, 1985.
8. Василенко, О.Н. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко. – М.: МЦНМО, 2003.
9. Виноградов, И.М. Основы теории чисел / И.М. Виноградов. – М.: Наука, 1976.
10. Каргополов, М.И. Основы теории групп / М.И. Каргополов, Ю.И. Мерзляков. – М.: Наука, 1972.
11. Конопелько, В.К. Прикладная теория кодирования / В.К. Конопелько, В.А. Липницкий [и др.] Т. 1-2. – Минск: БГУИР, 2004.
12. Коутинхо, С. Введение в теорию чисел. Алгоритм RSA / С. Коутинхо. – М.: Постмаркет, 2001.
13. Ленг, С. Алгебра / С. Ленг. – М.: Мир, 1968.
14. Лиддл, Р. Конечные поля / Р. Лидл, Г. Нидеррайтер. Т. 1-2. – М.: Мир, 1988.
15. Мак-Вильямс, Ф.Дж. Теория кодов, исправляющих ошибки / Ф.Дж. Мак-Вильямс, Н.Дж.А. Слоэн. –М.: Связь, 1979.
16. Мальцев, А.И. Алгебраические системы / А.И. Мальцев. – М.: Наука, 1970.
17. Муттер, В.М. Основы помехоустойчивой телепередачи информации / В.М. Муттер. – Л.: Энергоатомиздат, 1990.
18. Ноден, П. Алгебраическая алгоритмика / П. Ноден, К. Китте. – М.: Мир, 1999.
19. Прасолов, В.В. Многочлены / В.В. Прасолов. –М.: МЦМНО, 2000.
20. Самсонов Б.Б. Теория информации и кодирование / Б.Б.Самсонов, Е.М. Плохов, А.И. Филоненков, Т.В. Кречет. – Р-н/ Д.: Феникс, 2002.
21. Серр, Ж.-П. Курс арифметики / Ж.-П. Серр. – М.: Мир, 1972.
22. Соловьев, Ю.П. Эллипические кривые и современные алгоритмы теории чисел / Ю.П. Соловьев, В.А. Садовничий, Е.Т. Шавгумидзе, В.В. Белокуров. – М. – Ижевск: Институт компьютерных исследований, 2003.
23. Сушкевич, А.К. Теория чисел. Элементарный курс / А.К. Сушкевич. – Харьков: ХГУ, 1954.
24. Черемушкин, А.В. Лекции по арифметическим алгоритмам в криптографии / А.В. Черемушкин. – М.: МЦНМЩ, 2002.
25. Харин Ю.С. Математические основы криптологии / Ю.С. Харин, В.И. Берник, Г.В. Матвеев. –Минск: БГУ, 1999.
26. Холл, М. Теория групп / М. Холл. – М.: Ил, 1962.