ОПРЕДЕЛЕНИЕ 3.8. *Разделить натуральное число n на натуральное число m (n ≥ m) с остатком это значит – найти такое* ***натуральное*** *число k и такое* ***неотрицательное целое*** число r, $0 \le r \le m - 1$, что

$$n = mk + r. \qquad (3\text{-}124)$$

Числа k и r называются соответственно ***частным*** *и* ***остатком*** *от деления n на m.* Если $r = 0$, то говорят, что n делится *нацело* на m и пишут: $m|n$.

END

Алгоритм Евклида состоит в следующем. Пусть n и m – положительные целые числа и $n \ge m$. Согласно выражению (3-124) найдём ряд равенств:

$$n = mk_1 + r_1, \quad 0 < r_1 < m,$$

$$m = r_1k_2 + r_2, \quad 0 < r_2 < r_1,$$

$$r_1 = r_2k_3 + r_3, \quad 0 < r_3 < r_2,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$

так как $n > m > r_1 > r_2 > \ldots \ge 0$, то найдётся неотрицательное целое $r_{s+1} = 0$, такое, что

$$r_{s-1} = r_sk_{s+1},$$

при этом несложно показать, что натуральное число r_s будет являться «m, n».

Определив «m, n» с помощью алгоритма Евклида, далее, не зная канонических разложений n и m, с помощью (3-122) можно определить $\langle m, n\rangle$.

ПРИМЕР 3.29. Найти НОД и НОК чисел n =13172 и m =257, не используя их канонических разложений.

Для определения «m, n» и $\langle m, n\rangle$ с учётом условий примера необходимо опираться на алгоритм Евклида и соотношение (3-122).

Согласно алгоритму Евклида

$$13172 = 51\cdot257\cdot + 65,$$

$$257\cdot = 3\cdot65 + 62,$$

$$65 = 1\cdot62 + 3,$$

$$62 = 20\cdot3 + 2,$$

$$3 = 1\cdot2 + 1,$$

$$2 = 2\cdot1 + 0;$$

таким образом, $r_{s-1} = r_6 = 0$ и согласно алгоритму Евклида

$$«m, n» = r_s = r_5 = 1;$$

согласно же соотношению (3-122)

$$\langle m, n\rangle = mn/«m, n» = mn/1 = 3385204.$$

END

ЦЕЛЫЕ ЧИСЛА

Множество всех целых чисел **есть множество всех натуральных чисел и дополнительно определяемых новых объектов – числа 0 и множества всех отрицательных целых чисел. Множество всех целых чисел обозначается символом** Z:

$$Z = \{0, \pm1, \pm2, \pm3, \ldots, \pm n, \ldots\}. \qquad (3\text{-}125)$$

Число нуль, обозначаемый символом 0, и *отрицательные целые числа* вводятся следующим образом.

Сумма любого натурального числа n и числа 0 есть n:

$$n + 0 = n. \qquad (3\text{-}126)$$

Любому *натуральному числу* n соответствует единственное *отрицательное целое число* $(-n)$, такое, что сумма чисел n и $(-n)$ равна нулю:

$$n + (-n) = 0. \qquad (3\text{-}127)$$

Числа n и $(-n)$ называются взаимно *противоположными*. Натуральные числа в множестве целых чисел называются *положительными целыми числами*.

Абсолютным значением (или *модулем*) целого числа n называется число, обозначаемое $|n|$ и вычисляемое по правилу:

$$|n| = \begin{cases} n, \text{ если } n > 0, \\ 0, \text{ если } n = 0, \\ -n, \text{ если } n < 0. \end{cases} \qquad (3\text{-}128)$$

Множество всех целых чисел является *упорядоченным* множеством: для любых двух целых чисел n и m имеет место одно и только одно из *следующих соотношений*:

$$n = m, \qquad n < m, \qquad n > m.$$

В множестве целых чисел вводятся арифметические операции: *сложение* и *умножение*, которые обозначаются соответственно символами + и · .

ОПРЕДЕЛЕНИЕ 3.9. ***Суммой*** *двух целых чисел n и m называется целое число q, вычисляемое по правилу*:

если $n > 0$ и $m > 0$, то $q = n + m$;
если $n < 0$ и $m < 0$, то $q = -(|n| + |m|)$;
если $n > 0$ и $m < 0$ и $|n| > |m|$, то $q = |n| - |m|$;
если $n > 0$ и $m < 0$ и $|n| = |m|$, то $q = 0$;
если $n > 0$ и $m < 0$ и $|n| < |m|$, то $q = (|n| - |m|)$;
если $n < 0$ и $m > 0$ и $|n| > |m|$, то $q = -(|n| - |m|)$;
если $n < 0$ и $m > 0$ и $|n| = |m|$, то $q = 0$;
если $n < 0$ и $m > 0$ и $|n| < |m|$, то $q = -(|n| - |m|)$;
если $n = 0$, то $q = m$;
если $m = 0$, то $q = n$.

Сумма q двух целых чисел n и m записывается с помощью символа +:

$$q = n + m. \qquad (3\text{-}129)$$

END

ОПРЕДЕЛЕНИЕ 3.10. ***Произведением*** *двух целых чисел n и m называется целое число q, вычисляемое по правилу*:

если $n > 0$ и $m > 0$, то $q = n \cdot m$;
если $n < 0$ и $m < 0$, то $q = |n| \cdot |m|$;
если $n < 0$ и $m > 0$, или если $n > 0$ и $m < 0$
то $q = -(|n| \cdot |m|)$;
если $n = 0$ или $m = 0$, то $q = 0$.

Произведение q двух целых чисел n и m записывается с помощью символа ·:

$$q = n \cdot m \quad \text{или} \quad q = nm. \qquad (3\text{-}130)$$

END

Вводятся также *операция вычитания целых чисел* и *операция деления целых чисел*.

С операциями сложения и вычитания связаны понятия: *сумма чисел*, *слагаемое*, *разность чисел*, *уменьшаемое*, *вычитаемое*.

С операциями *умножения* и *деления* связаны понятия: *произведение чисел*, *сомножитель*, *частное* (*целых чисел*), *делимое*, *делитель*, *натуральная степень числа*.

Множество всех целых чисел *замкнуто* относительно операций сложения, вычитания и умножения, так как сумма, разность и произведение любых двух целых чисел являются также целыми числами.

Множество всех целых чисел *не замкнуто* относительно операции деления, так как эта операция не всегда имеет результат в множестве всех целых чисел.

Операция сложения подчинена правилам *коммутативности и ассоциативности*.

Операция умножения подчинена правилам *коммутативности и ассоциативности*.

Операции сложения и умножения целых чисел связаны *законом дистрибутивности умножения относительно сложения* (см. табл. 2.1).

Частным от деления целого числа n на целое число m называется целое число q такое, что

$$n = mq. \qquad (3\text{-}131)$$

При этом о целом числе q говорят, что оно является результатом деления *нацело* числа n на число m, и пишут

$$q = n/m; \qquad (3\text{-}132)$$

о m и q говорят, что они являются делителями n, а о n говорят, что оно является *числом* ***кратным*** *числу* m (или числу q).

Во избежание возникновения неопределённости при делении целых чисел запрещается деление на число 0.

Не для каждой пары целых чисел n и m найдется такое целое число q, что будет выполняться (3-131). Например, при $n = -7$ и $m = 2$ такое целое число q не существует.

Целое число $p \geq 1$, которое делится только на $\pm p$ и ± 1, называется *простым*.

НОК двух целых чисел m и n называется *наименьшее целое* ***положительное*** *число*, кратное каждому из этих чисел; НОК двух целых чисел m и n обозначается как $\langle m, n \rangle$.

НОД двух целых чисел m и n называется *наибольшее целое* ***положительное*** *число*, являющееся делителем каждого из этих чисел; НОД двух целых чисел m и n обозначается как «m, n».

Говорят, что два целых числа *взаимно просты*, если их НОД равен 1.

СРАВНЕНИЯ

Для изложения всего материала настоящего подраздела потребуется ввести *операцию деления целого числа на натуральное число с остатком*.

ОПРЕДЕЛЕНИЕ 3.11. *Разделить* ***целое число*** a ***на натуральное число*** m *с остатком это значит найти такое* ***целое число*** k *и такое* ***неотрицательное целое число*** r, $0 \leq r \leq m - 1$, что

$$a = mk + r. \qquad (3\text{-}133)$$

Числа k *и* r *называются соответственно* ***частным*** *и* ***остатком*** *от деления* a *на* m.

END

Например, при $a = -11$ и $m = 2$ имеем: $k = -6$, $r = 1$.

Целые числа a и b называются *равноостаточными* или *сравнимыми по модулю* m (m – ***натуральное число*** – *модуль*), если их разность $(a - b)$ делится на m *без остатка*; этот факт выражают записью

$$(a - b) \equiv 0 \pmod{m}, \qquad (3\text{-}134)$$

или

$$a \equiv b \pmod{m}, \qquad (3\text{-}135)$$

что читается так: «a сравнимо с b по модулю m». Таким образом, «сравнение по модулю m» (3-135) представляет собою соотношение между тремя числами, где a и b называются *левой и правой частями сравнения* соответственно, а m выполняет роль эталона сравнения.

Очевидно, что из (3-133) следует

$$a \equiv r \pmod{m}, \qquad (3\text{-}136)$$

что означает, что всякое целое число a сравнимо со своим вычетом по модулю m; при этом $r \in \{0, 1, \ldots, m - 1\}$.

Легко показать что, если $a \equiv r_1 \pmod{m}$ и $b \equiv r_2 \pmod{m}$, то $a \equiv b$ в том и только в том случае, когда $r_1 = r_2$.

В теории чисел доказывается, что ряд свойств сравнений по одинаковому модулю m (m – произвольное натуральное число) аналогичны свойствам равенств:

так отношение сравнимости обладает свойствами рефлексивности ($a \equiv a \pmod{m}$), симметричности (если $a \equiv b \pmod{m}$, то $b \equiv a \pmod{m}$) и транзитивности (если $a \equiv b \pmod{m}$ и $b \equiv c \pmod{m}$, то $a \equiv c \pmod{m}$);

правую и левую части сравнения можно умножать на одно и то же произвольное целое число; сравнения можно складывать, перемножать и т.д.

ПРИМЕР 3.30. Просто доказываются следующие свойства сравнений.

1) Если $a \equiv b \pmod{m}$ и k – произвольное натуральное число, то $ka \equiv kb \pmod{km}$.

2) Если $a \equiv b \pmod{m}$ и k – произвольное целое число, то $ka \equiv kb \pmod{m}$.

3) Если $ka \equiv kb \pmod{m}$ и $\langle\langle k, m \rangle\rangle = 1$, то $a \equiv b \pmod{m}$.

4) Если $ka \equiv kb \pmod{km}$, где k и m – произвольные натуральные числа, то $a \equiv b \pmod{m}$.

5) Если $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, то $a + c \equiv b + d \pmod{m}$ и $a - c \equiv b - d \pmod{m}$.

6) Если $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, то $ac \equiv bd \pmod{m}$.

7) Если $a \equiv b \pmod{m}$, то при любом целом $n \geq 0$ $a^n \equiv b^n \pmod{m}$.

8) Если $a + b \equiv c \pmod{m}$, то $a \equiv c - b \pmod{m}$.

Сравнения в представленном эдесь виде впервые были введены Гауссом в его книге «Disquisitiones arithmeticae» («Исследования по арифметике», 1801 г.).

END

ОПРЕДЕЛЕНИЕ 3.14. *Классом по данному модулю m называется множество всех целых чисел* $\{a\}$, *сравнимых по модулю m с некоторым неотрицательным целым числом* $r \in \{0, 1, \ldots, m\text{-}1\}$.

END

Обозначим класс всех целых чисел, сравнимых по модулю m с r, через

$$\bar{r} = \{a | a \equiv r \pmod{m}\}. \qquad (3\text{-}137)$$

Очевидно, что все целые числа, принадлежащие классу $\bar{r}$, можно получить, заставив целое число t пробегать все возможные значения из множества всех целых чисел $\{0, \pm1, \pm2, \pm\ldots\}$ в выражении:

$$a = ml + r. \qquad (3\text{-}138)$$

Любое число класса называется *вычетом* по модулю m по отношению ко всем остальным числам этого же класса. Поэтому иногда класс по модулю m называют классом вычетов по модулю m. Вычет, получаемый при $l = 0$, равный самому остатку r, называется *наименьшим неотрицательным вычетом*.

Взяв от каждого класса по одному вычету, получим *полную систему вычетов по модулю m*. Наиболее часто в качестве полной системы вычетов используют наименьшие неотрицательные вычеты 0, 1, …, m-1; в данной книге делается также.

Очевидно, что каждый класс вычетов по модулю m имеет бесконечное число элементов, а число различных классов вычетов по модулю m равно m:

$$\overline{0},\ \overline{1},\ \ldots,\ \overline{m-1}\ . \qquad (3\text{-}139)$$

Также ясно, что введённые классы вычетов попарно не пересекаются, а каждое целое число попадает в один и только в один класс.

Введём в множестве классов вычетов по модулю m две операции, которые будут называться *сложением* и *умножением* классов; при этом результатом сложения является *сумма классов*, а результатом умножения – *произведение классов*.

Действительно, пусть $\overline{r_1}$ и $\overline{r_2}$ – два класса вычетов, а a_1 и a_2 – *произвольные числа* из этих классов: $a_1 \in \overline{r_1}$, $a_2 \in \overline{r_2}$.

Суммой классов $\overline{r_1}$ и $\overline{r_2}$ называется класс $\overline{r_1 + r_2}$, т.е. класс, содержащий число $a_1 + a_2$:

$$\overline{r_1} + \overline{r_2} = \overline{r_1 + r_2}\ . \qquad (3\text{-}140)$$

Произведением классов $\overline{r_1}$ и $\overline{r_2}$ называется класс $\overline{r_1 r_2}$, т.е. класс, содержащий число $a_1 a_2$:

$$\overline{r_1} \cdot \overline{r_2} = \overline{r_1 r_2}\ . \qquad (3\text{-}141)$$

При таком определении операций сложения и умножения классов вычетов получается алгебраическая система, имеющая множество m элементов – всевозможных классов вычетов по модулю m: $\{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$, над которыми определены две бинарные операции – сложение и умножение.

Очевидно, что множество m всевозможных классов вычетов по модулю m с введёнными бинарными операциями сложения и умножения классов является коммутативным кольцом с нулевым элементом относительно сложения $\overline{0}$ и с единичным элементом относительно умножения $\overline{1}$; обозначим это кольцо через Z_m.

Важно подчеркнуть, что если порядок кольца целых чисел Z равен бесконечности, то порядок Z_m является конечным и равным m.

Мы будем называть для краткости сложением по модулю 2 двух целых чисел α и β процедуру определения остатка r в выражении:

$\alpha + \beta = 2t + r \equiv r \pmod 2$, где t – целое число,

а r будем называть суммой $\alpha + \beta$ по модулю 2; иногда для краткости вместо последнего выражения будем писать

$$\alpha \oplus \beta = r.$$

3.19. ЗАДАЧИ

3.1. Чему равно число различных многочленов степени k и меньше над полем порядка p?

3.2. Пусть $g(X) \in F_0[X]$ – некоторый неприводимый многочлен степени m. Чему равно число классов вычетов в $F_0[g]$?

3.3. Пусть I_n – число двоичных неприводимых многочленов степени n. Существует ли такое n, при котором $I_n = 0$? Какими сведениями Вы располагаете по этому вопросу?

3.4. Доказать, что ожидаемое число неприводимых делителей случайно выбранного многочлена достаточно большой степени n над конечным полем порядка q приблизительно равно $\ln n$.

3.5. Показать, что элементы поля $F_0[g]$ α^{m-1}, α^{m-2}, …, 1 образуют базис в A_m, где m – степень неприводимого многочлена $g(X)$, с помощью которого создано поле $F_0[g]$.

3.6. Решить уравнение второго порядка над $GF(2)$: $g(X) = X^2+X+1 = 0$. В том случае, если оно не имеет решений в поле $GF(2)$, найти корни этого уравнения, расширив соответствующим образом поле $GF(2)$.

3.7. Убедиться, что многочлен $g(X) = X^3+X^2+1$ является неприводимым в поле $GF(2)$. Построить поле $GF(3^2)$, используя для этого неприводимый многочлен $g(X)$.

3.8. Поле $GF(2^3)$ можно получить как с помощью неприводимого многочлена X^3+X+1, так и с помощью неприводимого многочлена X^3+X^2+1. Получить таблицу соответствия представлений элементов.

3.9. Найти примитивные элементы поля Z_p простого порядка в случае, если $p = 3, 5, 7$ (при $p=7$ имеются два примитивных элемента 3 и 5).

3.10. Построить таблицу сложения и умножения элементов поля $GF(7)$. Найти порядок каждого элемента. Какие элементы являются примитивными?

3.11. Найти все неприводимые двоичные многочлены степени 5 или меньше над полем $GF(2)$. Заметим, что если многочлен степени m не является неприводимым, то он обладает делителем, степень которого не превосходит $m/2$.

3.12. Сколько существует идеалов в алгебре многочленов по модулю X^6-1 над полем $GF(2)$? Перечислите порождающие их многочлены.

3.13. Рассмотрим мультипликативную циклическую группу числового поля Z_7. Очевидно, что её порядок равен 6, а элементами являются положительные целые числа 1, 2, 3, 4, 5, 6 – представители классов вычетов по mod 7. Найдите порядок каждого элемента группы и попытайтесь выписать все подгруппы этой группы.

3.14. Показать, что в векторном пространстве наборов длины n с элементами из $GF(2)$ любая подгруппа по сложению является подпространством.

3.15. Пусть $g(X) = g_m X^m+g_{m-1}X^{m-1}+ \ldots +g_0$ – порождающий многочлен циклического кода. Показать, что $g_0 \neq 0$.

3.16. Пусть $F_0 = GF(2)$, а $F_0[X]$ – множество всех многочленов над полем F_0. В $F_0[X]$ введены операции сложения и умножения многочленов и умножения многочленов на элементы из F_0.

Пусть $f(X)$ – многочлен степени n из $F_0[X]$ и рассматривается алгебра многочленов A_n по модулю $f(X)$.

Требуется:

1) перечислить все названия алгебраических структур, которыми является A_n, если многочлен $f(X)$ не является неприводимым многочленом в $F_0[X]$;

2) перечислить все названия алгебраических структур, которыми является A_n, если многочлен $f(X)$ является неприводимым многочленом в $F_0[X]$.

3.17. Показать, что в случае линейного (n, k)-кода кодовое расстояние $d_{мин} \le n\text{-}k+1=r+1$.

3.18. Кодом Рида-Соломона называется БЧХ-код с $m_0=1$. Показать, что для всех кодов Рида-Соломона выполняется соотношение: $d_{мин} = n\text{-}k+1=r+1$.

3.19. Построить умножитель произвольного входного многочлена на фиксированный многочлен $g(X) = X^3+X^2+1$.

3.20. Построить делители входного многочлена на многочлен:

1) $g_1(X) = X^3+X+1$,

2) $g_2(X) = X^3+X^2+1$.

Проверить работу схем делителей на примере входного полинома $d(X)=X^5+X^4+X^3+X+1$.

3.21. Представить ненулевые элементы $GF(2^4)$ как степени примитивного элемента α, зафиксированного с помощью многочлена X^4+X+1; затем степени примитивного элемента α представить как многочлены от α по модулю $\alpha^4+\alpha+1$ и определить минимальные многочлены для ненулевых элементов поля.

3.22. Продолжение задачи 3.21.

Существует ли связь между минимальными многочленами элементов поля $GF(2^4)$, созданного с помощью многочлена X^4+X+1, и числовыми циклами, представляющими последовательности степеней примитивного элемента α и описывающим некоторые подмножества элементов $GF(2^4)$?

3.23. Рассмотреть поле $GF(2^4)$ многочленов по модулю X^4+X+1. Найти многочлены этого поля, принадлежащие подполю $GF(2^2)$.

3.24. Найти порождающий многочлен для двоичного БЧХ-кода длины 15, исправляющего двукратные ошибки.

3.25. Найти порождающий многочлен для двоичного БЧХ-кода длины 15, исправляющего трёхкратные ошибки.

3.20. ВЫВОДЫ

В данном разделе были изложены теоретические основы построения класса циклических кодов и, в частности, его важнейшего подкласса – БЧХ-кодов. Полное овладение этим материалом позволит читателю уже без изъятий читать профессиональную литературу по теории кодирования и тем самым позволит приблизить возможность работы в этой интересной и важной области.

К новым результатам здесь относится описание работы умножителей и делителей многочленов с помощью их линейных эквивалентов.

Большое внимание было уделено вооружению читателя этой книги профессиональным инструментарием для выбора и анализа свойств циклических кодов при решении конкретных задач кодирования, помещённые в V разделе книги:

Приложение 5.2. Разложение бинома X^n+1 на неприводимые биномы над полем $GF(2)$,

Приложение 5.3. Некоторые функции ядра и основной библиотеки математической системы Maple V R5,

Приложение 5.4. Таблица разложения бинома X^n+1 на неприводимые сомножители над $GF(2)$,

Приложение 5.5. Таблица циклических (n, k)-кодов,

открывают читателю широкие возможности такого рода деятельности.

Уделено значительное внимание описанию свойств кодирующих устройств циклических кодов.

3.21. ЛИТЕРАТУРА

Основная

3.1. Галлагер Р. Теория информации и надёжная связь. М.: Советское радио, 1974.

3.2. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. М.: Мир, 1976.

3.3. Касами Т., Токура Н., Ивадари Ё и др. Теория кодирования. М.: Мир, 1978.

3.4. Берлекэмп Э. Алгебраическая теория кодирования. М.: Мир, 1971.

3.5. Бухштаб А.А. Теория чисел. М.: Учпедгиз, 1960.

3.6. Виноградов И.М. Основы теории чисел. М.: Наука, 1972.

3.7. Постников М.М. Теория Галуа. М.: Факториал Пресс. 2003.

3.8. Биркгоф Г., Барти Т. Современная прикладная алгебра. М.: Мир, 1976.

3.9. Курош А.Г. Курс высшей алгебры. М.: Физматгиз, 1963.

3.10. Элементы теории передачи дискретной информации. / Под общей ред. Л.П. Пуртова. М.: Связь, 1972.

3.11. Блейхут Р. Теория и практика кодов, контролирующих ошибки. М.: Мир, 1986.

Дополнительная

3.12. Теория кодирования : Пер. с англ. Сборник работ в области математической теории кодирования. М.: Мир,1964.

3.13. Яглом А.М., Яглом И.М. Вероятность и информация. М.: Наука, 1973.

3.14. Цыпкин А.Г. Справочник по математике для средних учебных заведений. М.: Наука, 1988.

3.15. Титце У., Л. Шенк. Л. Полупроводниковая схемотехника. М.: Мир, 1982.

3.16. Хоровитц П., Хилл У. Искусство схемотехники. Т. 2. : Пер. с англ. М.: Мир, 1993.

3.17. Теория автоматического регулирования. Ч.1. / Под ред. А.А. Воронова М.: Высшая школа, 1986.

3.18. Панин В.В. Основы теории информации. Ч.1. М.: МИФИ, 2001.

3.19. Говорухин В.Н., Цибулин В.Г. Введение в Maple. Математический пакет для всех. М.: Мир, 1997.

3.20. Дьяконов В.П. Математическая система MAPLE V R3/R4/R5. М.: «СОЛОН», 1998.

3.21. Херхагер М., Партолль Х. Mathcad 2000. Полное руководство : Пер. с немец. под ред. К.Ю. Королькова. Киев: «Ирина», BHV, 2000.

3.22. Кондрашов В.Е., Королёв С.Б. MATLAB как система программирования научно-технических расчётов. М.: Мир, 2002.

3.23. Дьяконов В.П., Абраменкова И.В. МАТЛАБ 5.0/5.3. Система символьной математики. М.: «Нолидж», 1999.

3.24. Свердлик М.Б. Оптимальные дискретные сигналы. М.: Советское радио, 1975.

3.25. Аршинов М.Н., Садовский Л.Е. Коды и математика. Серия: библиотечка «Квант». М.: Наука, 1983.

3.26. Гольденберг Л.М. и др. Цифровая обработка сигналов. Справочник. М.: Радио и связь, 1985.