6. ТЕОРИЯ ЧИСЕЛ И НЕКОТОРЫЕ ЕЕ ПРИЛОЖЕНИЯ

Одним из разделов дискретной математики является теория чисел, которая первоначально изучала свойства целых чисел. Целое число является одним из древнейших математических понятий, связанных с подсчетом окружающих предметов. Теория чисел возникла из задач арифметики и первоначально оперировала четырьмя арифметическими действиями над натуральными (целыми, положительными) числами. Основными понятиями этой теории являлись *простые числа*, *составные числа*, *квадратные числа* (числа, равные квадрату некоторого другого числа), *совершенные числа* (число, равное сумме своих делителей). В 6 в. до н. э. в Древней Греции было известно решение уравнения $x^2 + y^2 = z^2$ в целых числах. В 3 в. до н. э. Евклид в «Началах» обосновал алгоритм нахождения наибольшего общего делителя двух произвольных целых чисел и доказал, что количество простых чисел является бесконечным. Эратосфен предложил метод нахождения простых чисел («Решето Эратосфена»). Систематизация проблем теории чисел и методов их решений была выполнена в 3 в. н. э. Диофантом в «Арифметике». В 17 в. н. э. Ферма исследовал решения многих уравнений в целых числах и высказал гипотезу, что уравнение $x^n + y^n = z^n$, $n>2$, x, y, z – целые, не имеет решений (великая теорема Ферма). Ему также принадлежит утверждение о том, что если a и p взаимно простые числа (наибольший общий делитель этих чисел равен 1), где a – целое, p – простое, то $a^p - a$ делится на p нацело (малая теорема Ферма). Эйлер доказал великую теорему Ферма при $n = 3$ и обобщил малую теорему Ферма, введя понятие функции $\varphi(m)$ – количества чисел ряда 1, 2, 3, ..., m взаимно простых с m, ныне называемую функцией Эйлера от целого m, и показал, что любое число a, взаимно простое с m, возведенное в степень $\varphi(m)$, при делении на m дает в остатке 1. Проблема нахождения целых положительных остатков при делении одного целого на другое возникла из задач календарных расчетов в Китае (Суньцзы, Цинь Цзюшао) и в современном виде формулируется как китайская теорема об остатках.

Важным понятием теории чисел являются сравнения, основные свойства которых были доказаны Гауссом. Сравнение является свойством эквивалентности чисел, имеющих одинаковые положительные остатки при делении на некоторое целое число – модуль.

Теория чисел тесно связана с другими разделами дискретной математики: теорией графов, комбинаторикой, теорией конечных автоматов, дискретным спектральным анализом и, конечно, с теорией дискретных групп. Так, множество чисел 0, 1, 2, ..., $p-1$ удовлетворяет аксиомам группы с операцией сложения по модулю p. Если считать p простым числом и исключить из множества 0, то оставшееся множество с операцией умножения по модулю p также образует группу. В этом случае множество чисел 0, 1, 2, ..., $p-1$ с двумя заданными на нем операциями сложения и умножения по модулю p образует числовое поле, которое называется полем Галуа и обозначается $GF(p)$ – сокращение от *Galois Field*. Галуа показал, что для любого простого p и целого h существует конечное поле с числом элементов, равным p^h. Такое поле обозначается $GF(p^h)$. Оно является для заданных p и h единственным (с точностью до изоморфизма). В любом поле $GF(p^h)$ в качестве подполя содержится поле $GF(p)$. Обычно поля Галуа вида $GF(p^h)$ не рассматриваются в теории чисел, однако логическая связь этих полей с числовыми полями $GF(p)$, похожие свойства полей и тесное переплетение в технических приложениях позволили рассмотреть их основные свойства в данном пособии.

6.1. Основные понятия и определения

Приведем некоторые определения и свойства целых чисел, которые потребуются для формулировки двух главных теорем теории чисел.

6.1.1. Делимость целых чисел

Что общего между числами множества 9, 16, 23, 30, 37, 44 кроме того, что они все целые? Казалось бы ничего. Однако, если ввести операцию деления с остатком и интересоваться только целым положительным остатком от деления чисел этого множества на 7, то окажется, что все они будут иметь одинаковый остаток, равный 2. Эти числа эквивалентны по этому свойству. Тогда приведенную последовательность можно продолжить дальше: 51, 58, 65, 72, 79... Это множество чисел является бесконечным и счетным, все числа множества объединяет одно общее свойство: при делении на 7 они дают целый положительный остаток 2. Говорят, что эти числа a сравнимы по модулю 7. Такое свойство множества обозначают $a \equiv 2 \bmod 7$.

Можно рассмотреть другое множество чисел, например 3, 12, 21, 30, 39, 49,..., и убедиться в том, что при делении на число 9 все они дают остаток 3, т. е. общее свойство чисел a этого множества можно записать так: $a \equiv 3 \bmod 9$.

Произвольное целое число a единственным образом может быть представлено в виде $a = mt + r$, где $m > 0$ – целое положительное число (делитель), t – частное, r – остаток ($0 \le r < m$). Так, например, если $a = 17$, $m = 5$, то $17 = 5 \cdot 3 + 2$.

В дальнейшем мы будем использовать операцию деления и интересоваться только остатком, не обращая внимание на частное. Так, например, число 16 при делении на 11 дает остаток 5.

Наименьший положительный остаток от деления некоторого числа a на число m обычно называют наименьшим неотрицательным вычетом a по модулю m. Если m делит a нацело, то остаток $r = 0$. Например, наименьший неотрицательный вычет при делении числа 18 на 6 равен 0.

Пусть имеется два числа a и b. Будем говорить, что они сравнимы по модулю m, если при делении на m они дают одинаковый целый положительный остаток. Например, числа 8 и 15 при делении на 7 имеют одинаковый остаток 1, т. е. они сравнимы по модулю 7. Сравнение чисел будем обозначать так: $a \equiv b \bmod m$.

Сравнению $a \equiv 0 \bmod m$ удовлетворяют все числа a, которые делятся на m нацело или, как говорят, кратные m.

6.1.2. Свойства сравнений

От сравнения $a \equiv b \bmod m$ можно перейти к равенству. Сравнение $a \equiv b \bmod m$ справедливо, если выполняется следующее равенство: $a = b + m \cdot t$, где $\cdot$ – умножение, t – некоторое целое (положительное, отрицательное или 0).

Такая связь между сравнениями и равенствами позволяет распространить понятие сравнения не только на положительные, но и на отрицательные числа. Например, можем записать $12 \equiv 7 \equiv 2 \equiv -3 \equiv -8 \equiv -13 \ldots \bmod 5$.

Из связи между сравнениями и равенствами следуют правила эквивалентных преобразований сравнений.

a) Если $a \equiv b \bmod m$ и $b \equiv c \bmod m$, то $a \equiv c \bmod m$.

b) Если $a \equiv b \bmod m$ и $c \equiv d \bmod m$, то $a+b \equiv c+d \bmod m$. Это правило можно сформулировать и так: сравнения по одинаковому модулю можно почленно складывать.

c) Если $a \equiv b \bmod m$, то $a \equiv b+m \cdot t \bmod m$, так как справедливо сравнение $m \cdot t \equiv 0 \bmod m$, т. е. к любой части сравнения можно прибавить модуль, умноженный на любое целое.

d) Если $a \equiv b \bmod m$ и c – любое целое, взаимно простое с m, то $a \cdot c \equiv b \cdot c \bmod m$, т. е. обе части сравнения можно умножить на любое целое, если оно взаимно простое с модулем m.

e) Если $a \equiv b \bmod m$ и c – любое целое, взаимно простое с m, то $a/c \equiv b/c \bmod m$, т. е. обе части сравнения можно разделить на любое целое, если оно взаимно простое с модулем m.

Последнее свойство позволяет распространить понятия сравнения и на дробные числа. Так, например, если имеем сравнение $1/3 \equiv 16/15 \bmod 11$, то так как (15, 11) = 1, т. е. числа 15 и 11 взаимно просты, то обе части сравнения можно умножить на 15, и получим эквивалентное сравнение: $5 \equiv 16 \bmod 11$.

6.1.3. Решение сравнений

Из приведенных правил эквивалентных преобразований сравнений следуют общие приемы решения сравнений. Пусть требуется решить сравнение $27 - 13 \cdot 5 \equiv 10 \cdot X \bmod 7$ относительно неизвестного X. Можно показать, что если в сравнении имеется арифметическое выражение, то любой член его можно заменить остатком от деления на модуль (в общем случае – на любое сравнимое с ним число). Так как $27 \equiv 6 \bmod 7$, $13 \equiv -1 \bmod 7$ и $10 \equiv 3 \bmod 7$, то исходное сравнение можно представить в виде $6 - (-1) \cdot 5 \equiv 3 \cdot X \bmod 7$.

Далее вычисляем $11 \equiv 3 \cdot X \bmod 7$, $18 \equiv 3 \cdot X \bmod 7$, $6 \equiv X \bmod 7$, откуда одно из решений сравнения – $X = 6$. Общее решение $X = 6 + t \cdot 7$.

Упражнения.

Найти общие решения следующих сравнений:

a) $8 \equiv 3X \bmod 11$;

b) $25 \equiv 15\ X \bmod 17$;

c) $3(24-18)/5 \equiv 7X \bmod 19$;

d) $8^{125} - 6^{29} \equiv 5X \bmod 7$;

e) $$\frac{(75 \cdot 1824 + 33 \cdot 2083)}{37 \cdot 21^6} \equiv 23^3\, X \bmod 19;$$

f) $$\frac{36 \cdot 10^{112} + 81 \cdot 12^{58}}{41 \cdot 9^{10}} \equiv 21^6 X \bmod 11.$$

6.1.4. Наименьшее общее кратное и наибольший общий делитель

Пусть имеется n целых чисел: $a_1, a_2, a_3, \ldots, a_n$. Общим кратным этих чисел называется целое число, которое делится нацело на каждое из этих чисел. Наименьшее из этих общих кратных называется наименьшим общим кратным чисел $a_1, a_2, a_3, \ldots, a_n$ и обозначается НОК ($a_1, a_2, a_3, \ldots, a_n$) или $[a_1, a_2, a_3, \ldots, a_n]$.

Пусть имеется n целых чисел $a_1, a_2, a_3, \ldots, a_n$. Общим делителем этих чисел называется число, которое нацело делит каждое их этих чисел. Сре-

ди делителей имеется наибольшее число, которое называется наибольшим общим делителем – НОД $(a_1, a_2, a_3, ..., a_n)$ или $(a_1, a_2, a_3, ..., a_n)$.

6.1.5. Простые числа. Разложение на простые сомножители. Каноническая форма числа

Число, которое не имеет никаких делителей, кроме 1 и самого себя, называется простым числом. Примеры простых чисел: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...

Любое число N может быть представлено в виде произведения степеней простых чисел (каноническое представление числа). Такое представление единственно (с точностью до перестановки сомножителей). Так, число $600 = 2^3 3^1 5^2$.

Для представления числа N в канонической форме можно использовать следующий алгоритм. Число N делим на наименьшее простое число 2 до тех пор, пока оно делится нацело, затем на 3, на 5 и т. д.

Например, $N = 10500$. $10500 : 2 = 5250$; $5250 : 2 = 2625$. Это число больше не делится на 2 нацело. Делим его на 3. $2625 : 3 = 875$. Это число на 3 нацело не делится. Делим его на 5. $875 : 5 = 175$. Еще раз делим на 5. $175 : 5 = 35$. Еще раз делим на 5. $35 : 5 = 7$. Число 7 – простое число, поэтому окончательно имеем в канонической форме: $10\,500 = 2^2 3^1 5^3 7^1$.

6.1.6. Определение НОК И НОД чисел

Для произвольного целого числа a и произвольного целого положительного числа b существуют такие числа t и r, что $a = bt + r$, где $0 \le r < b$. Причем такое представление единственное.

Можно показать, что если $b|a$ (b делит a нацело), то $(a, b) = b$, и если $a = bt + r$, то $(a, b) = (b, r)$.

Для нахождения наибольшего общего делителя двух чисел a и b известен алгоритм Евклида: пусть $a \ge b$. Рассмотрим следующую последовательность равенств:

$$a = bt_1 + r_2,\ 0 < r_2 < b;$$
$$b = r_2 t_2 + r_3,\ 0 < r_3 < r_2;$$
$$r_2 = r_3 t_3 + r_4,\ 0 < r_4 < r_3 \ ...$$
$$r_{n-1} = r_n t_n + r_{n+1},\ 0 = r_{n+1}.$$

Поскольку $a \ge b > r_2 > r_3 > ... \ge 0$, то алгоритм имеет конечное число шагов. Согласно вышеприведенным свойствам, $(a, b) = (b, r_2) = (r_2, r_3) = ... = r_n$. Таким образом, наибольший общий делитель чисел a и b равен последнему ненулевому остатку в последовательности равенств, т. е. r_n. А наименьшее общее кратное a и b равно $[a, b] = ab/(a, b)$.

Упражнения.

Используя алгоритм Евклида, найти НОК и НОД чисел:

а) 575 и 155;

β) 840 и 188650;

с) 4851 и 29106;

d) 975 и 616.

Если два числа N_1 и N_2 представлены в канонической форме соответственно: $N_1 = p_1^{n_1} p_2^{n_2} \dots p_s^{n_s}$, $N_2 = p_1^{m_1} p_2^{m_2} \dots p_s^{m_s}$, то

$$\text{НОК}\left(N_1, N_2\right) = p_1^{\min(n_1, m_1)} p_2^{\min(n_2, m_2)} p_s^{\min(n_s, m_s)};$$

$$\text{НОД}\ \left(N_1, N_2\right) = p_1^{\min(n_1, m_1)} p_2^{\min(n_2, m_2)} p_s^{\min(n_s, m_s)}.$$

Если в каноническом представлении одного из чисел отсутствует какой-либо простой сомножитель, его можно ввести в нулевой степени. Например, для чисел $N_1 = 2^3 5^2 7^1$ и $N_2 = 3^1 5^1 11^2$, прежде чем находить НОК и НОД, требуется их привести к одинаковой форме, т. е. сделать так, чтобы в каноническом представлении обоих чисел присутствовали бы одинаковые простые числа в соответствующих степенях, а именно: $N_1 = 2^3 3^0 5^2 7^1 11^0$; $N_2 = 2^0 3^1 5^1 7^0 11^2$. Тогда НОК ($N_1$, N_2) = $= 2^3 3^1 5^2 7^1 11^2 = 508200$, НОД ($N_1$, N_2) = $2^0 3^0 5^1 7^0 11^0 = 5$.

Упражнения.

Найти НОК и НОД для пар чисел:

а) $N_1 = 440$; $N_2 = 6050$;

β) $N_1 = 234$; $N_2 = 4125$;

с) $N_1 = 66550$; $N_2 = 40131$;

d) $N_1 = 388$; $N_2 = 1647$.

Приведенный алгоритм легко обобщается на произвольное количество чисел, для которых требуется определить НОК и НОД.

Упражнения.

Найти НОК и НОД для следующих наборов чисел:

а) $N_1 = 60$; $N_2 = 350$; $N_3 = 495$;

β) $N_1 = 265$; $N_2 = 104$; $N_3 = 93$;

с) $N_1 = 2100$; $N_2 = 630$; $N_3 = 5880$; $N_4 = 9450$;

d) $N_1 = 700$; $N_2 = 495$; $N_3 = 104$;

е) $N_1 = 103$; $N_2 = 260$; $N_3 = 121$.

6.1.7. Функция Эйлера для натурального числа φ(m)

Функция Эйлера $\varphi(m)$ определяется для всех целых чисел m как количество чисел ряда 1, 2, 3, ..., m взаимно простых с m. Так, $\varphi(1) = 1$ (по определению), $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$ и т. д. Легко показать, что для $m = p$ (простых чисел) $\varphi(p) = p-1$. Для $m = p^n$ функция

Эйлера $\varphi(p^n) = p^{n-1}(p-1)$. Для произвольного числа m, представленного в канонической форме $m = p_1^{n_1} p_2^{n_2} \dots p_s^{n_s}$, функция Эйлера определяется следующим образом: $\varphi(m) = m(1-1/p_1)(1-1/p_2)\dots(1-1/p_s)$.

Например: $\varphi(11) = 10$; $\varphi(9) = 6$; $\varphi(18) = 6$.

Упражнения.

Вычислить функцию Эйлера $\varphi(m)$ для чисел m = 7, 12, 15, 17, 23, 24, 25, 28, 37, 54, 64.

6.1.8. Сравнимость чисел и классы вычетов

Выпишем все числа от 1 до 8 и вычеркнем все числа не взаимно простые с 8. Количество оставшихся чисел равно $\varphi(m = 8) = 4$, а сами эти числа (1, 3, 5, 7). Множество этих чисел обладает свойством замкнутости относительно операции умножения по модулю $m = 8$. Действительно, перемножая любые пары чисел из множества (1, 3, 5, 7) и находя наименьший положительный остаток по модулю $m = 8$, будем получать всегда одно из этих же чисел. Каждое из этих чисел порождает бесконечный счетный класс чисел: $1+8\cdot t$; $3+8\cdot t$; $5+8\cdot t$; $7+8\cdot t$, где t – любое целое.

Более того, множество классов с порождающими элементами в виде этих чисел обладает свойством замкнутости, а именно: при любых целых t произведение представителей классов ($1+8\cdot t$; $3+8\cdot t$; $5+8\cdot t$; $7+8\cdot t$) дает в результате представителя одного из этих же классов.

Можно показать, что классы вычетов, получаемые в соответствии с функцией Эйлера, всегда образуют абелеву группу по умножению. А это, в частности, означает, что для любого представителя из этих классов можно найти обратный элемент из представителей этих же классов.

Упражнения.

Постройте абелевы группы классов, порождаемые числами 10, 12, 15, 18, 21, 24, 25, 27, 28.

6.1.9. Теоремы Ферма и Эйлера

Теорема Ферма.

Существует мнение, что Ферма не публиковал свои научные труды, а формулировал свои знаменитые теоремы либо в письмах к знакомым математикам, либо на полях рукописей. Так, на полях одной из рукописей Ферма написал, что если p – простое число и $(a, p) = 1$, то $a^{p-1} \equiv 1 \bmod p$.

Пусть $p = 23$, $a = 18$. Очевидно, что (23, 18) = 1, следовательно, $18^{22} \equiv 1 \bmod 23$. Проверить этот результат несложно. Для этого заметим, что $18 \equiv -5 \bmod 23$, поэтому можно написать эквивалентное сравнение: $(-5)^{22} \equiv 1 \bmod 23$ или $5^{22} \equiv 1 \bmod 23$. Последнее сравнение можно представить в виде $(5^2)^{11} \equiv 1 \bmod 23$, и так как $25 \equiv 2 \bmod 23$, то

$2^{11} \equiv 1 \bmod 23$. Полученное сравнение элементарно проверяется: $2048 \equiv 1 \bmod 23$.

Теорема Эйлера.

Если $m > 1$ и $(a, m) = 1$, то $a^{\varphi(m)} \equiv 1 \bmod m$. Эта теорема обобщает теорему Ферма, так как при $m = p$, $\varphi(m = p) = p - 1$.

Пусть $m = 18$, $a = 5$. Очевидно, что $(5, 18) = 1$.

Функция Эйлера $\varphi(m = 18) = 6$. Поэтому $5^6 \equiv 1 \bmod 18$. Это сравнение проверяется достаточно просто: $5^2 \equiv 7 \bmod 18$, следовательно, $((5^2))^3 \equiv 7^3 = 343 \equiv 1 \bmod 18$.

Упражнения.

На основании теорем Ферма и Эйлера доказать справедливость сравнений:

a) $2^{36} \equiv 3^{36} \equiv \ldots \equiv 36^{36} \equiv 1 \bmod 37$;

b) $2^{100} \equiv 3^{100} \equiv \ldots \equiv 100^{100} \equiv 1 \bmod 101$;

c) $2^8 \equiv 4^8 \equiv 7^8 \equiv 8^8 \equiv 11^8 \equiv 13^8 \equiv 14^8 \equiv 1 \bmod 15$.

6.1.10. Показатели чисел по модулю и примитивные корни

Пусть $(a, m) = 1$. Рассмотрим бесконечную последовательность степеней числа a: $a^0 = 1$, a^1, a^2, a^3, ... В соответствии с теоремой Эйлера существует целое положительное число s, такое, что

$$a^s \equiv 1 \bmod m. \qquad (6.1)$$

В самой теореме $s = \varphi(m)$. Могут существовать и другие целые положительные числа s, удовлетворяющие этому сравнению. Наименьшее из них обозначается $\boldsymbol{e}$ и называется показателем числа a по модулю m. Иногда $\boldsymbol{e}$ называют порядком числа a по модулю m.

Набор степеней числа a вида a^0, a^1, a^2, a^3, ..., a^{e-1} попарно несравнимы между собой по модулю m. Докажем это. Пусть, например, при некоторых n_1 и n_2 выполняется сравнение $a^{n_1} \equiv a^{n_2} \bmod m$, где для определенности $n_1 < n_2 < \boldsymbol{e}$. Умножим обе части сравнения на a^{e-n_2}, тогда получим $a^{(e+n_1-n_2)} \equiv 1 \bmod m$. Но поскольку $n_1 < n_2$, то в левой части сравнения степень числа a меньше $\boldsymbol{e}$, что противоречит тому, что $\boldsymbol{e}$ – наименьшее число, удовлетворяющее сравнению (6.1). Если найдется некоторое k, такое, что $a^k \equiv 1 \bmod m$, то $\boldsymbol{e}$ является делителем k. Очевидно, что всегда e является делителем $\varphi(m)$.

Пример.

Возьмем $m = 45$, $a = 2$, $(45, 2) = 1$. Функция Эйлера $\varphi(45) = 24$, следовательно, $2^{24} \equiv 1 \bmod 45$. Число 24 представляется в канонической форме в виде $24 = 2^3 3$, т. е. имеет 8 разных делителей: 1, 2, 3, 4, 6, 8, 12, 24. Проверка показывает, что наименьшее число $e = 12$, так как $2^{12} \equiv 1 \bmod 45$.

Если показатель ***e*** числа a по модулю m равен $\varphi(m)$, то a называют примитивным элементом по модулю m.

Пример. По каким модулям число $a = 2$ является примитивным элементом? $m = \mathbf{3}, \mathbf{5}, 7, \mathbf{9}, \mathbf{11}, 15, 17, \mathbf{19}$.

6.1.11. Конечные поля (поля Галуа)

В разд. 3 приведены определения математических моделей с одним классом объектов – групп, колец и полей (в частности – полей Галуа).

Можно показать, что числовое конечное поле (поле с конечным числом элементов) существует только при операциях сложения и умножения по модулю p, где p – простое число. Такие поля называются числовыми конечными полями Галуа и обозначаются $GF(p)$ или $F(p)$.

Примеры.

1. Построить конечные поля $F(2)$, $F(3)$, $F(7)$. Для решения этих примеров указать все элементы множества U, найти нейтральные и обратные элементы для групп по сложению и умножению с соответствующим модулем.

2. Показать, что не существует полей $F(6)$, $F(12)$, $F(15)$.

Поля Галуа можно построить в совершенно другой форме, а именно как поля многочленов по модулю некоторого неприводимого многочлена над числовым полем $F(p)$. В этом случае порядок поля (число его элементов) равен p^h, где p – простое, h – целое.

Пусть $F(p)$ – числовое поле Галуа порядка p. Рассмотрим множество многочленов вида

$$f(X) = a_0 + a_1X + a_2X^2 + \ldots + a_kX^k,$$

где $a_i \in F(p)$, $i = 0, 1, 2, 3\ldots, k$, т. е. коэффициенты принимают значения из $F(p)$, операции сложения и умножения чисел выполняются по $\bmod p$. Если $a_k \neq 0$, то многочлен $f(X)$ имеет степень k. Множество всех многочленов, имеющих степень k и меньше, будем обозначать $F^{(k)}[X]$.

Введем операции сложения и умножения многочленов над полем $F(p)$ следующим образом. Пусть

$$f(X) = \sum f_iX^i \text{ и } g(X) = \sum g_iX^i.$$

Тогда

$$f(X) + g(X) = \sum_i (f_i + g_i)X^i;\ f(X)\cdot g(X) = \sum_i \left(\sum_{j=0} f_i g_{i-j} \right) X^i.$$

Например: пусть

$$f(X) = f_0 + f_1 X;\ g(X) = g_0 + g_1 X + g_2 X^2.$$

Тогда

$$f(X) + g(X) = (f_0 + g_0) + (f_1 + g_1)X + g_2 X^2;$$
$$f(X) \cdot g(X) = (f_0 g_0) + (f_0 g_1 + f_1 g_0)X + (f_1 g_1 + f_0 g_2)X^2 + f_1 g_2 X^3.$$

Отсюда видно, что при сложении степень результирующего многочлена равна максимальной степени слагаемых, а при умножении – сумме степеней перемножаемых многочленов.

Упражнения.

Сложить и перемножить следующие пары многочленов:

a) $f(X) = f_0 + f_1 X + f_2 X^2;\ g(X) = g_0 + g_1 X + g_3 X^3;$

b) $f(X) = f_1 X + f_2 X^2 + f_5 X^5;\ g(X) = g_0 + g_1 X^1 + g_4 X^4;$

c) $f(X) = f_1 X + f_2 X^2 + X^5;\ g(X) = g_0 + g_1 X^3 + g_2 X^4.$

А теперь сделайте то же самое, если указано **конечное** числовое поле (модуль):

d) $f(X) = 2X + 3X^2 + X^5;\ g(X) = 4 + 2X^3 + X^4,\ p = 7;$

e) $f(X) = 3X + 2X^2 + 2X^5;\ g(X) = 2 + 4X^1 + 3X^4,\ p = 5.$

Если рассматривать многочлены всех возможных степеней $F(X)$, то с такими операциями сложения и умножения множество многочленов образует кольцо.

Для любых двух многочленов $f(X)$ и $g(X)$ существуют, и притом единственные, многочлены $a(X)$ и $r(X)$, такие, что $f(X) = a(X)g(X) + r(X)$, где степень $g >$ степени r. Переходя к сравнениям многочленов, получаем

$$f(X) \equiv r(X) \bmod (g(X)). \qquad (6.2)$$

Деление многочленов производится так же, как и деление целых чисел. Следует только учитывать, что все операции выполняются в поле $F(p)$. Например, разделим многочлен $g(X) = 1 + X + X^2$ на $f(X) = 1 + X$ в поле $F(2)$:

$(1 + X + X^2)$	$(1 + X)$
$X + X^2$	X
1	

В результате получим $(1 + X + X^2) : (1 + X) = X$, при этом в остатке будет 1. Для деления удобнее записывать многочлены в обратном порядке, начиная со старшей степени. При вычислении в поле $F(2)$ операция сложения имеет специальное обозначение «$\oplus$» и называется «сложение по модулю 2».

Упражнения.

Найти остатки от деления многочленов:

а) $X^5 \oplus X^2 \oplus X$ на $X^3 \oplus X^2 \oplus X \oplus 1$ в поле $F(2)$ **(0)**

b) $2X^4 + X^2 + 2$ на $X^3 + 2X^2 + 2X + 1$ в поле $F(3)$ **($2X^2$)**

Если в (6.2) остаток $r(X) = 0$, то говорят, что $g(X)$ делит $f(X)$. Если в $F(X)$ нет ни одного многочлена степени, большей 0, который бы делил $f(X)$ без остатка, за исключением скалярных кратных $f(X)$, т. е. многочленов вида $bf(X)$, где $b \in F(p)$, то многочлен $f(X)$ называется *неприводимым*.

Найдем неприводимые многочлены некоторых малых степеней.

Имеется два многочлена первой степени: $X \oplus 1$ и X. По определению, они оба считаются неприводимыми.

Многочлен второй степени вида $X^2 \oplus aX \oplus b$ будет неприводимым над полем $F(2)$, если он не будет делиться ни на какой неприводимый многочлен первой степени, т. е. ни на $X \oplus 1$, ни на X. А это означает, что он не должен иметь корней в поле $F(2)$. Таким образом: $F(0) = b \neq 0$, $F(1) = 1 \oplus a \oplus b \neq 0$. Откуда получаем, что $a = 1$, $b = 1$, а сам неприводимый многочлен 2-го порядка имеет вид $X^2 \oplus X \oplus 1$.

Многочлен третьей степени имеет общий вид $X^3 \oplus aX^2 \oplus bX \oplus c$. Он будет неприводимым в поле $F(2)$, если не будет делиться ни на один из неприводимых многочленов первой степени (проверять делимость на многочлен второй степени не требуется). Таким образом, должны выполняться условия: $F(0) = c = 1$, $F(1) = 1 \oplus a \oplus b \oplus 1 = 1$. Следовательно, либо a, либо b должны равняться 1, но не оба вместе, поэтому существуют два неприводимых многочлена третьей степени: $X^3 \oplus X^2 \oplus 1$ и $X^3 \oplus X \oplus 1$.

Приведем табл. 6.1 всех неприводимых многочленов над полем $F(2)$, степень которых не превышает 4.

Возьмем один из неприводимых многочленов степени 2 над числовым полем $F(2)$, например $X^2 \oplus X \oplus 1$. При делении на этот многочлен все многочлены будут давать остатки (вычеты по модулю этого неприводимого многочлена). Приведем все виды остатков: $\{(0), (1), (X), (X \oplus 1)\}$. Каждый из этих остатков образует класс вычетов по модулю неприводимого многочлена, а их совокупность с операциями сложения и умножения по модулю неприводимого многочлена образует поле. Порядок этого поля (число элементов) в общем случае может быть равен p^h, где p – про-

Таблица 6.1

Максимальная степень многочлена	Неприводимые многочлены в поле $F(2)$
1	$X \oplus 1$; X
2	$X^2 \oplus X \oplus 1$
3	$X^3 \oplus X^2 \oplus 1$; $X^3 \oplus X \oplus 1$
4	$X^4 \oplus X^3 \oplus X^2 \oplus X \oplus 1$; $X^4 \oplus X \oplus 1$; $X^4 \oplus X^3 \oplus 1$

стое, h – целое. В приведенном примере $p = 2$, $h = 2$ и порядок поля равен 4.

Упражнение.

Постройте поля Галуа $F(2^3)$, $F(2^4)$ для пяти полиномов (многочленов), взятых из табл. 6.1.

Элемент поля α, такой, что $F(\alpha) = 0$, называется корнем многочлена $f(X)$. В этом случае говорят, что уравнение $f(X)$ имеет корень в поле $F(p)$.

Упражнения.

a) Найдите корни многочлена $X^2 + X + 1$ в полях $F(2)$, $F(3)$, $F(5)$, $F(7)$.

Покажем, как это сделать для поля $F(5)$. В уравнение

$$X^2 + X + 1 = 0 \qquad (6.3)$$

будем последовательно подставлять значения элементов поля: 0, 1, 2, 3, 4. В результате получим:

$$0^2 + 0 + 1 \equiv 1 \bmod 5;$$
$$1^2 + 1 + 1 \equiv 3 \bmod 5;$$
$$2^2 + 2 + 1 \equiv 2 \bmod 5;$$
$$3^2 + 3 + 1 \equiv 3 \bmod 5;$$
$$4^2 + 4 + 1 \equiv 1 \bmod 5,$$

т. е. этот многочлен не имеет корней в поле $F(5)$. Однако он имеет корни в поле $F(7)$. Действительно, при $X = 2$ и $X^2 = 4$ левая часть уравнения (6.3) обращается в 0.

b) Найдите корни многочлена X^4+X^3+1 в тех же полях, что и в примере 1.

Конечное поле $F(p^h)$ содержит p^h элементов. Основное поле $F(p)$, которое является подполем поля $F(p^h)$, содержит p элементов (0, 1, 2, 3,..., $p-1$) и 2 операции: $\oplus \bmod p$ и $\otimes \bmod p$.

Элемент α называется алгебраическим степени h над полем $F(p)$, если и только если α удовлетворяет в $F(p)$ уравнению $P(x) = 0$, где $P(x)$ – многочлен степени h, но не удовлетворяет никакому уравнению с многочленом меньшей степени. Это влечет неприводимость многочлена $P(x)$. Все p^h элементов поля $F(p^h)$ могут быть представлены в виде $\sum c_j \alpha^i$, где $0 \le c_j \le p-1$; $0 \le \alpha^i \le h-1$. При вычислениях степень α^s, где $s \ge h$, заменяется на меньшую в соответствии с уравнением $P(\alpha) = 0$.

Пусть, например, $p = 3$, $h = 2$ и α удовлетворяет уравнению $x^2 - x - 1 = 0$. Элементы поля $F(3^2)$ можно выразить как 0, 1, 2, α, $\alpha + 1$, $\alpha + 2$, 2α, $2\alpha + 1$, $2\alpha + 2$.

В вычислениях понижение степеней производится с использованием равенства $\alpha^2 = \alpha + 1$. Например: $(2\alpha + 1)(\alpha + 2) = 2\alpha^2 + \alpha + 4\alpha + 2 = 2(\alpha + 1) + 5\alpha + 2 = 7\alpha + 4 = \alpha + 1$.

Элемент $\beta \neq 0$ поля $F(p^h)$ называется образующей $F^*(p^h)$ мультипликативной группы ненулевых элементов поля $F(p^h)$, если степени β^i, $i = 1, 2, 3, \ldots, p^h - 1$ пробегают все ненулевые элементы поля $F(p^h)$. Образующая может рассматриваться как основание log. Такие логарифмы называются дискретными логарифмами. Рассмотрим, например, все 8 степеней (кроме нулевой) корня α в приведенном выше примере и запишем результат в виде таблицы:

i	1	2	3	4	5	6	7	8
α^i	α	$\alpha + 1$	$2\alpha + 1$	2	2α	$2\alpha + 2$	$\alpha + 2$	1

Из таблицы видно, что α является образующей. Эта таблица может быть представлена как таблица дискретных логарифмов. Для этого в верхней строке запишем упорядоченные элементы поля, а в нижней – значения степеней образующего элемента, при которых получаем данный элемент поля:

y	1	2	α	$\alpha + 1$	$\alpha + 2$	2α	$2\alpha + 1$	$2\alpha + 2$
$\log_\alpha y$	8	4	1	2	7	5	3	6

Считается, что вычисление дискретных логарифмов является трудной задачей, как и задача факторизации (разложения на множители), что является существенным в криптосистемах с открытым распределением ключей. Таблица логарифмов может использоваться для выполнения умножения и деления элементов поля. Заметим, что операции выполняются по модулю $p^h - 1$, в данном примере – по модулю $3^2 - 1 = 8$.

Для примера: $\log((\alpha + 2)(2\alpha + 1)) = \log(\alpha + 2) + \log(2\alpha + 1) = 7 + 3 = 10 \equiv 2 \bmod 8$. Что соответствует элементу $\alpha + 1$. $\log((\alpha + 1)/(2\alpha + 2)) = 2 - 6 = -4 \equiv 4 \bmod 8$, что соответствует элементу 2.

Можно проверить, что кроме элемента α образующими β также являются элементы $2\alpha + 1$, $\alpha + 2$ и 2α. Если $s = p^h - 1$ есть наименьшая положительная степень, удовлетворяющая уравнению $\beta^s = 1$, то β является образующей. Поэтому число образующих элементов поля равно $\varphi(p^h - 1)$, где φ – функция Эйлера. Для нашего примера $\varphi(8) = 4$.

Упражнения.

Найдите количество образующих элементов для полей Галуа: $F(3^4)$, $F(5^2)$, $F(7^2)$, $F(11^5)$, $F(13^4)$.

6.1.12. Квадратичные вычеты. Символ Лежандра. Символ Якоби

Рассмотрим поле Галуа $F(p^h)$ при $p > 2$ и h – целом. Исключим из элементов поля нулевой элемент, а оставшееся множество обозначим $F^*(p^h)$. Если некоторый элемент $a \in F^*(p^h)$ есть квадрат некоторого элемента $x \in F^*(p^h)$, то a называют *квадратичным вычетом*, если же такого элемента x не найдется в $F^*(p^h)$, то a называют *квадратичным невычетом*.

Пример. Рассмотрим поле $F(3^2)$. Все элементы поля можно представить в виде 0, 1, 2, α, $\alpha + 1$, $\alpha + 2$, 2α, $2\alpha + 1$, $2\alpha + 2$, где α – корень некоторого неприводимого полинома степени 2 над полем $F(3)$. Возьмем в качестве такого полинома $P(X) = X^2 - X - 1$. Тогда $P(\alpha) = \alpha^2 - \alpha - 1 = 0$. При выполнении вычислений будем производить замену: $\alpha^2 = \alpha + 1$. $F^*(3^2)$ будет содержать все те же элементы, кроме элемента 0, а именно: 1, 2, α, $\alpha + 1$, $\alpha + 2$, 2α, $2\alpha + 1$, $2\alpha + 2$. Будем последовательно возводить в квадрат все элементы поля (кроме нулевого) и выявлять квадратичные вычеты:

$$1^2 = \mathbf{1};\ 2^2 = 1;\ \alpha^2 = \boldsymbol{\alpha + 1};\ (\alpha + 1)^2 = \alpha^2 + 2\alpha + 1 = \alpha + 1 + 2\alpha + 1 = \mathbf{2};$$
$$(\alpha + 2)^2 = \alpha^2 + 4\alpha + 4 = (\alpha + 1) + 4\alpha + 4 = \boldsymbol{2\alpha + 2};\ (2\alpha)^2 = 4\alpha^2 = (\alpha + 1);$$
$$(2\alpha + 1)^2 = 4\alpha^2 + 4\alpha + 1 = \alpha + 1 + 4\alpha + 1 = 2\alpha + 2;$$
$$(2\alpha + 2)^2 = 4\alpha^2 + 8\alpha + 4 = \alpha^2 + 2\alpha + 1 = 2.$$

Таким образом элементы 1, 2, $\alpha = 1$ и $2\alpha + 2$ являются квадратичными вычетами, а остальные элементы α, $\alpha + 2$, 2α и $2\alpha + 1$ – квадратичными невычетами.

Упражнения.

Найдите квадратичные вычеты и квадратичные невычеты в полях Галуа: $F(3^3)$, $F(5^2)$.

Пусть теперь $h = 1$. Рассмотрим поле $F(p)$ с элементами 0, 1, 2,..., $p-1$. Если исключить элемент 0, то для остальных элементов поля можно также определить, являются они квадратичными вычетами или невычетами. Ясно, что элемент a, $1 \le a \le p-1$ будет квадратичным вычетом по модулю p тогда и только тогда, когда выполняется сравнение $x^2 \equiv a \bmod p$, где x также является элементом поля $F(p)$.

Пример. Пусть $p = 7$. Тогда $1^2 \equiv \mathbf{1} \bmod 7$; $2^2 \equiv \mathbf{4} \bmod 7$; $3^2 \equiv \mathbf{2} \bmod 7$; $4^2 \equiv 2 \bmod 7$; $5^2 \equiv 4 \bmod 7$; $6^2 \equiv 1 \bmod 7$. Таким образом, квадратичными вычетами являются числа 1, 2, 4, а квадратичными невычетами – числа 3, 5, 6.

Если a – квадратичный вычет по модулю p, полученный возведением в квадрат числа x, то это же число будет получено возведением в квадрат числа $-x \equiv p - x \bmod p$. Поэтому все квадратичные вычеты по

модулю p можно найти возведением в квадрат чисел 1, 2, 3,..., $(p-1)/2$. Таким образом, для любого p имеется ровно $(p-1)/2$ квадратичных вычетов и столько же квадратичных невычетов.

Упражнения.

Найдите квадратичные вычеты и квадратичные невычеты по простым модулям $p = 11, 13, 17, 19, 23$.

Символ Лежандра для целого a и простого $p > 2$ определяется следующим образом:

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

Понятно, что a можно заменить любым целым числом, сравнимым с a по модулю p, при этом символ Лежандра не изменится. Вычисление символа Лежандра удобно производить по формуле

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \bmod p.$$

Действительно:

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

Упражнения.

Вычислите следующие символы Лежандра:

$$\left(\frac{7}{5}\right), \left(\frac{3}{7}\right), \left(\frac{11}{7}\right), \left(\frac{35}{11}\right), \left(\frac{169}{13}\right), \left(\frac{523}{13}\right).$$

Символ Якоби является обобщением символа Лежандра на случай произвольного нечетного модуля $n > 2$. Пусть число n представлено в канонической форме: $n = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$. Тогда символ Якоби определяется как произведение символов Лежандра:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{s_1} \left(\frac{a}{p_2}\right)^{s_2} \dots \left(\frac{a}{p_k}\right)^{s_k}.$$

Например, пусть $n = 363\,825 = 3^3 5^2 7^2 11^1$. Найдем символ Якоби для числа $a = 863$. Сначала найдем наименьший положительный вычет числа 863 по модулям $p = 3$, 5, 7 и 11:

$$863 \equiv 2 \bmod 3;\ 863 \equiv 3 \bmod 5;\ 863 \equiv 2 \bmod 7;\ 863 \equiv 5 \bmod 11.$$

Тогда символ Якоби можно вычислить следующим образом:

$$\left(\frac{863}{363825}\right)=\left(\frac{863}{3}\right)^3\left(\frac{863}{5}\right)^2\left(\frac{863}{7}\right)^2\left(\frac{863}{11}\right)^1=\left(\frac{2}{3}\right)^3\left(\frac{3}{5}\right)^2\left(\frac{2}{7}\right)^2\left(\frac{5}{11}\right)^1=$$

$$=(2^1\equiv -1 \bmod 3)^3\,(3^2\equiv -1 \bmod 5)^2\,(2^3\equiv 1 \bmod 7)^2\,(5^5\equiv 1 \bmod 11)^1=$$

$$=(-1)(1)(1)(1)=-1,$$

т. е. число 863 является квадратичным невычетом по модулю 363825.

Для произведения чисел выполняется свойство мультипликативности:

$$\left(\frac{ab}{n}\right)=\left(\frac{a}{n}\right)\left(\frac{b}{n}\right).$$

Тогда

$$\left(\frac{abb}{n}\right)=\left(\frac{a}{n}\right)\left(\frac{b}{n}\right)\left(\frac{b}{n}\right)=\left(\frac{a}{n}\right).$$

Для некоторых значений a символ Якоби вычисляется без перевода n в каноническую форму следующим образом:

$$\left(\frac{1}{n}\right)=1;\ \left(\frac{-1}{n}\right)=(-1)^{(n-1)/2};\ \left(\frac{2}{n}\right)=(-1)^{(n^2-1)/8}.$$

При вычислении символа Якоби основное сведение выполняется на основе закона взаимности:

$$\left(\frac{m}{n}\right)=(-1)^{(m-1)(n-1)/4}\left(\frac{n}{m}\right),$$

где m и n – нечетные числа, большие двух.

Если не выполняется сравнение $m \equiv n \equiv 3 \bmod 4$, то

$$\left(\frac{m}{n}\right)=\left(\frac{n}{m}\right).$$

Если же это сравнение выполняется, то

$$\left(\frac{m}{n}\right)=-\left(\frac{n}{m}\right).$$

Пример. Определить, является ли число $a = 369$ квадратичным вычетом или квадратичным невычетом по модулю 247?

$369 \equiv 1 \bmod 4$, поэтому можно вычислить:

$$\left(\frac{369}{247}\right)=\left(\frac{122}{247}\right)=\left(\frac{247}{122}\right)=\left(\frac{3}{122}\right)=\left(\frac{122}{3}\right)=\left(\frac{122}{3}\right)=-1,$$

т. е. 369 является квадратичным невычетом по модулю 247.

Упражнения.

Определить символы Якоби в следующих случаях:

a) $\left(\frac{1815}{1683}\right)$; b) $\left(\frac{361}{5515}\right)$; c) $\left(\frac{2197}{625}\right)$.

Для криптографических систем представляет интерес случай, когда n является произведением двух простых чисел p и q, т. е. $n = pq$. Требуется определить, является ли некоторое число a квадратичным вычетом или квадратичным невычетом по модулю n, т. е. существует ли такое x, что выполняется сравнение $x^2 \equiv a \bmod n$?

Некоторое число a будет квадратичным вычетом по модулю $n = pq$, если и только если оно будет квадратичным вычетом как по модулю p, так и по модулю q. Если рассмотреть множество чисел 1, 2, 3,..., $n-1$ и исключить из него все числа, кратные p и (или) q, то в точности половина из оставшихся чисел будет удовлетворять условию $\left(\frac{a}{n}\right)=1$, а вторая половина будет удовлетворять условию $\left(\frac{a}{n}\right)=-1$. Более того, из чисел a, удовлетворяющих условию $\left(\frac{a}{n}\right)=1$, половина будет квадратичными вычетами, а именно такие числа a, для которых $\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=1$. Другая половина, для которых $\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=-1$, будет квадратичными невычетами.

Пример. Пусть $p = 3$, $q = 5$, тогда $n = 15$. Квадратичными вычетами по модулю 15 будут числа $a = 1$ и 4. Квадратичными невычетами будут числа $a = 2$ и 8.

Если известно, что некоторое a является квадратичным вычетом по модулю $n = pq$, но простые числа p и q неизвестны, то решение сравнения (нахождение x из сравнения) $x^2 \equiv a \bmod n$ является важной, но очень сложной задачей в криптографии с открытым ключом.