Лекция 14

Вычисления в модулярной арифметике

План лекции:

1) Целые числа по модулю m

2) Греко-китайская теорема об остатках

3) Арифметика вычетов

1) Целые числа по модулю m

**Замечание**. При фиксированном m > 1 по определению (см. лекцию 6) b ≡ m a тогда и только тогда, когда b – a = m \* q для некоторого q (иными словами, тогда и только тогда, когда m делит (b – a)).

**Замечание**. Формулы b ≡ m a и b ≡ a (mod m) являются синонимами (читаются: «b равно a по модулю m» или «b сравнимо с a по модулю m»). Обозначения предложены Гауссом.

**Замечание**. Множество классов эквивалентности Z / ≡ m , которое обозначается также Z m , называется множеством вычетов или целыми числами по модулю m .

**Замечание**. Важнейшие алгебраические свойства целых чисел верны и для целых чисел по модулю m .

**Свойства отношения эквивалентности ≡ m**

Теорема.

А. Если a ≡ b (mod m) и d делит m , то a ≡ b (mod m) .

B. Если a ≡ b (mod m) и a ≡ b (mod n) , то a ≡ b ( mod [m , n] ) .

C. Если a ≡ c (mod m) и b ≡ d (mod m) , то :

a + b ≡ c + d (mod m)

a – b ≡ c – d (mod m)

a \* b ≡ c \* d (mod m)

D. (свойство сокращения) Если a \* b ≡ a \* c (mod m) , то b ≡ c (mod m / d) , где

d = ( a , m ) . В частности, если ( a , m ) = 1 , то a \* b ≡ a \* c (mod m) влечёт за собой b ≡ c (mod m)

**Конгруэнция ≡ m**

Мы имеем сюръективное отображение : s : Z → Z m

Положим : a + b = s (a + b); a \* b = s (a \* b)

Из предыдущей теоремы вытекает, что это определение корректно, т.е. если c ∈ a и d ∈ b – другие представители, получаем:

s (c + d) = s (a + b); s (c \* d) = s (a \* b)

Таким образом, отношение эквивалентности ≡ m сохраняет алгебраически свойства (в частности, операции сложения и умножения), т.е. является конгруэнцией.

**Модулярные арифметики**

Используя свойство евклидовости, можно рассматривать арифметику целых чисел по модулю m как арифметику остатков или модулярную арифметику. Полная система остатков по модулю m состоит из m целых чисел, по одном представителю из каждого класса эквивалентности.

Наиболее часто используются две следующие системы:

(1) **система неотрицательных** остатков по модулю m , состоящая из чисел 0 , 1 , 2 , … , m – 1

(2) система наименьших по абсолютной величине остатков (**симметричная система** остатков), состоящая из чисел 0 , ± 1 , ± 2 , … , ± (m – 1)/2 для нечётного числа m .

**Конгруэнтность целых чисел**

Запишем целое число a следующим образом: a = m \* q + r , где 0 ≤ r ≤ m.

Остаток r (который обозначается также в виде r m (a) или r (a)), называется остатком по модулю m .

Утверждение. Два целых числа конгруэнтны тогда и только тогда, когда они имеют одинаковые остатки по модулю m (т.е. используя введённые обозначения:

b ≡ a (mod m) ⇔ r m (a) ≡ r m (b))

Для целого числа a его класс эквивалентности : a = a + m Z является в точности множеством чисел, остатки которых совпадают с r (a) .

Остатки 0 , 1 , 2 , … , m – 1 являются представителями классов эквивалентности, поэтому иногда отождествляют класс эквивалентности с представляющим его остатком и рассматривают Z m просто как множество { 0 , 1 , … , m – 1 }.

**Проблема обратных элементов в Z m**

Числами в модулярной арифметике являются остатки по модулю m .

Противоположный (**аддитивный обратный**) элемент к произвольному числу a ∈ Z m всегда существует и равен m – a . **Мультипликативный обратный** элемент к a ∈ Z m ,определяемый как решение следующего уравнения a \* x ≡ 1 (mod m) существует не всегда.

Теорема. Пусть a ∈ Z m .Тогда a имеет мультипликативный обратный элемент по модулю m в том и только в том случае, когда ( a , m ) = 1.

Доказательство : С помощью расширенного алгоритма Евклида можно найти целые числа x и y такие, что ( a , m ) = a \* x + m \* y , откуда вытекает, что a \* x ≡ ( a , m ) (mod m).

Если ( a , m ) = 1, то предыдущее сравнение означает, что x является мультипликативным обратным к a по модулю m . Если же ( a , m ) > 1 , то не существует числа x , для которого выполняется сравнение a \* x ≡ 1 (mod m) , т.к. a \* x = 1 + k \* m влечёт ( a , m ) = 1 .

**Z m – это кольцо или поле ?**

Теорема. Для всякого целого числа m > 1 множество Z m = { 0 , 1 , … , m – 1 } с операциями сложения и умножения по модулю m является коммутативным кольцом с единицей и называется кольцом вычетов по модулю m . Оно является полем тогда и только тогда, когда m – простое число.

Доказательство : С помощью определённого ранее сюръективного отображения s : Z → Z m , а также определения сложения и умножения в Z m , можно легко вывести, что Z m является коммутативным кольцом с единицей, из того, что Z является таким кольцом.

Пусть теперь m – простое число. Тогда все ненулевые элементы в Zm обратимы и, следовательно, является Z m полем. С другой стороны, если m не является простым, то Zm –не поле. Чтобы убедиться в этом,запишем : m=a \* b , a < m , b < m.

Тогда s (a) \* s (b) = s (m) = s (0), но s (a) ≠ s (0) и s (b) ≠ s (0) , откуда вытекает, что s (a) и s (b) являются делителями нуля.

**Примеры колец и полей Z m**

Пример 1. Кольцо Z 5 = { 0 , 1 , 2 , 3 , 4 }

является полем, т.к. все его ненулевые элементы 1 , 2, 3, 4 обратимы (обратные к ним элементы – это 1 , 3, 2, 4 соответственно).

Пример 2.

Кольцо Z 8 = { 0 , 1 , 2 , 3 , 4 , 5, 6 , 7 }

полем не является, т.к. в нём есть делители нуля ( например, 2 \* 4 = 0 (mod 8) ).

Теорема. Характеристика конечного поля – простое число.

**Вычисление a-1 в Z m**

1) малая теорема Ферма (см. лекцию 12),которая утверждает, что если m – простое число и a – произвольное целое число, не делящееся на m , то a m – 1 ≡ 1 (mod m)

2) следствие из малой теоремы Фермы, которое утверждает, что если m – простое число, то в кольце Z m выполняется равенство a – 1 = a m – 2

(3) теорема Эйлера, обобщающая малую теорему Ферма (m – не обязательно простое число),которая утверждает, что если ( a , m ) = 1 , то a φ (m) ≡ 1 (mod m)

(4) следствие из теоремы Эйлера, которое утверждает, что в кольце Z m из

( a , m ) = 1 следует, что a – 1 = a φ (m) – 1

Для вычисления мультипликативного обратного к a по модулю m элемента нужно возвести a в некоторую степень k , которая равна либо m – 2 , либо φ (m) – 1 .

**Методы возведения в степень**

**Классический метод** возведения числа a в степень k , требует выполнения k умножений.

**Бинарный метод**, является более эффективным. Запишем k в двоичной системе счисления,опустив нули перед первой значащей цифрой : k = Σ k i 2 i для всех

0 ≤ i ≤ n – 1 , где n – разрядность двоичного представления.

Заменим каждую цифру «1» на строку «SM a » (SM – означает Square + Multiply)

и каждую цифру «0» на строку «S» (S – означает Square). После этого вычеркнем слева строку «SM a ». Таким образом, получилась последовательность букв, которая представляет собой правило для вычисления a k , если интерпретировать «S» как «возвести в квадрат и взять остаток по модулю m», а «M a » как «умножить на a и взять остаток по модулю m».

Замечание. Процедура бинарного метода работает слева направо по отношению к битовому представлению числа k . Однако удобнее работать справа налево, т.к. в этом случае умножение на 2 – это просто сдвиг вправо на один разряд.

2) Греко-китайская теорема об остатках

**Группа обратимых элементов**

Обратимые элементы кольца Z m образуют мультипликативную группу, которая называется группой обратимых элементов кольца (или группой единиц кольца) Z m.

Эта группа обозначается U m = { a : ( a, m ) = 1 } и имеет φ (m) элементов.

Пусть G – группа из n элементов, a ∈ G и S = { k ≥ 1 : a k = e }. Т.к. a n = e , то S – не пусто. Кроме того S имеет наименьший элемент k 0 , который называется **порядком элемента** a .

Группа называется **циклической**, если в ней существует элемент a , степени которого ( 1 , a , a 2 , … ) пробегают все элементы группы.

Этот элемент называется образующим или, в случае группы U m , **примитивным корнем по модулю m** .

**Свойство цикличности группы U m**

Замечание. Можно показать, что порядок любого элемента группы U m делит φ (m).

Замечание. Примитивные корни, если они существуют, являются в точности элементами максимального возможного порядка φ (m) .

Теорема. Группа U m является циклической тогда и только тогда, когда m равно 1 , 2 , 4 , p a или 2 p a , где p – нечётное простое число и a > 0 .

Следствие. Если m – нечётное простое число, то группа U m циклическая и уравнение x 2 = 1 в U m не имеет решений, отличных от x = ± 1.

Замечание. Найдя примитивный корень a по модулю m в U m , можно получить другой корень – мультипликативно обратный a – 1 по модулю m .

**Уравнения по модулю m**

Теорема. Уравнение a \* x ≡ b (mod m) имеет решение тогда и только тогда, когда

( a , m ) | b .

Если решение существует, то оно единственно по модулю m / d , где d = ( a , m ); по модулю m уравнение имеет d решений.

**Пример**. Найдём решение уравнения 270 \* x ≡ 36 (mod 342)

Применяя расширенный алгоритм Евклида, получим : (– 5) \* 270 + 4 \* 342 = 18 (\*)

Уравнение имеет решение, единственное по модулю 19 = 342 / 18.

Для нахождения этого решения умножим равенство (\*) на 2 = 36 / 18 :

(– 10) \* 270 + 8 \* 342 = 36

Отсюда следует, что (– 10) – одно из решений уравнения по модулю 342. Другими решениями по модулю 342 являются числа 9 , 28 , 47 , 66 , 85 , 104 и т.д. Единственное решение по модулю 19 равно 9, т.к. 9 ≡ (– 10) (mod 19).

Следствие: Уравнение a \* x ≡ 1 (mod m) имеет решение тогда и только тогда, когда ( a , m ) = 1 .

Решение a – 1 (mod m) единственно по модулю m и является мультипликативным обратным к a элементом по модулю m .

**Пример**. Уравнение 2 \* x ≡ 1 (mod 26) не имеет решений, т.к. ( 2 , 26 ) = 2

В данном случае это можно показать и более простым способом : мы ищем число x , такое, что : 2 \* x – 1 = k \* 26.

**Теорема (греко-китайская теорема об остатках)**

Пусть m 1 , m 2 , … , m k – попарно взаимно простые целые числа > 1 и пусть M = m 1 \* m 2 \* … \* m k . Тогда существует единственное неотрицательное решение по модулю M следующей системы уравнений : x ≡ a 1 ( mod m 1 )

. . . . . . . . . . . . . .

x ≡ a k ( mod m k )

Другими словами, отображение, которое каждому целому числу x , 0 ≤ x ≤ M – 1 ставит в соответствие строку (a 1 , a 2 , … , a k), где x ≡ a i (mod m I) , i = 1 , 2 , .. , k является биекцией кольца Z M на Z m 1 x Z m 2 x … x Z m k.

**Пример.** Решим систему уравнений :

x ≡ 1 ( mod 2 )

x ≡ 2 ( mod 5 )

x ≡ 5 ( mod 7 )

x = 1 + 2 \* q

1 + 2 \* q ≡ 2 ( mod 5 ) или 2 \* q ≡ ( 2 – 1 ) ( mod 5 )

Теперь вычислим мультипликативный обратный элемент к 2 ( mod 5 ),который = 3.

Таким образом, имеем : q ≡ 3 ( mod 5 ) или q = 3 + 5 \* r для некоторого r.

Следовательно, решением первых двух уравнений является :

x = 1 + 2 \* ( 3 + 5 \* r ) = 7 + 2 \* 5 \* r , т.е. x ≡ 7 ( mod 2 \* 5 ).

Вход: Выход:

a , m 1, b , m 2 , такие, что x – единственное наименьшее

x ≡ a ( mod m 1 ) , x ≡ b ( mod m 2 ) неотрицательное решение по модулю

m 1 , m 2 – короткие целые числа m 1 \* m 2 системы сравнений :

такие, что ( m 1 , m 2 ) = 1 , x ≡ a ( mod m 1 )

m 1 > 1 , m 2 > 1 x ≡ b ( mod m 2 )

[ Если a > 0 , то ничто не меняется ]

x : = MOD ( a , m 1 ) // MOD ( a , b ) – подпрограмма вычисления

// неотрицательного остатка от деления a на b

[ Вычисление m – 1 ]

m – 1 : = MODINV ( m 1 , m 2 ) // MODINV ( a , b ) – подпрограмма вычисления

// наименьшего неотриц.-го обратного элемента

// по модулю b к элементу a

[ Вычисление q ]

q : = MOD ( ( m – 1 ) \* ( b – x ) , m 2 )

[ Выход ]

Вернуть x : = x + m 1 \* q // Т.к. 0 ≤ q < m 2 , то возвращаемое значение x

// удовлетворяет неравенствам 0 ≤ x < m 1 \* m 2

3) Арифметика вычетов

Замечание 1. Арифметика вычетов (остатков) – АВ является средством выполнения точных арифметических операций над ( длинными ) целыми числами.

Замечание 2. Основная идея обеспечения точности вычислений состоит в использовании операций над вычетами (для представления которых требуется существенно меньшая разрядность) вместо операций над целыми числами.

Замечание 3. В зависимости от отношения значений исходных целых чисел и допустимых значений модулей, с помощью которых формируются вычеты, применяется либо одномодульная, либо многомодульная арифметики.

**Одномодульная АВ – однозначность**

Отношение эквивалентности res ≡ res m ( mod m ) не определяет однозначно окончательный результат вычисления. Для того, чтобы определить res однозначно, нужно иметь априорную оценку его величины. Эта оценка используется в качестве модуля m и все операции выполняются в кольце Z m .

Если мы имеем оценку величины res ,то мы ищем наименьшее неотрицательное решение уравнения res ≡ res m ( mod m ). Если мы имеем оценку не величины res , а только величины | res | ,то мы ищем наименьшее по абсолютной величине решение.

Замечание. Для вычисления как положительных и отрицательных значений выражения можно использовать симметричную систему вычетов

Z p = { – (p – 1) / 2 , … , – 2 , – 1 , 0 , 1 , 2 , … , (p – 1) / 2 } ,

которая изоморфна системе неотрицательных вычетов Z p + ={ 0 , 1 , 2 , … , p – 1 }.

Однако обычно все операции АВ производятся в Z p + (Z p обеспечивает только интерфейс с Z).

**Операция деления**: Т.к. в конечном поле обратный элемент к любому ненулевому элементу всегда существует, деление по модулю p определяется следующим образом : a / b ( mod p) = a \* ( b – 1 ( mod p) ) ( mod p ), где b – 1 ( mod p) – это мультипликативный обратный элемент к элементу b по модулю p .

Частное двух целых чисел a и b в GF ( p ) также является целым числом, даже если b не делит a в Z .

Пусть модуль p ограничивает по величине окончательный результат res .

Возможны два случая :

(1) Если res ∉ GF ( p ) , то res p ≠ res; (2) Если res ∈ GF ( p ) , то res p = res

**Пример**. Выполним точные арифметические операции в GF (11). Чтобы вычислить значение x = 1 / 3 – 4 / 3 воспользуемся априорной информацией о том, что мы ищем результат в симметричной системе вычетов.

x ( mod 11 ) ≡ ( 1 / 3 + ( – 4 ) / 3) ( mod 11 )

≡ ( 1 / 3 + 7 / 3 ) ( mod 11 ) ----- в неотрицательной системе вычетов

≡ ( 1 \* 3 – 1 + 7 \* 3 – 1 ) ( mod 11 ) -- 3 – 1 является мультипликативным обратным элементом к 3 ( mod 11 )

≡ ( 1 \* 4 + 7 \* 4 ) ( mod 11 )

≡ 32 ( mod 11 )

Отображая результат обратно в симметричную систему вычетов, x = – 1.

Замечание. В приведённом выше примере res p = res , т.к. априорно известно, что res ∈ GF (p) и res принадлежит симметричному множеству.

**Стандартный набор остатков**

Общеизвестные системы счисления (например, десятичная) являются линейными, позиционными и весовыми. Вместо этого многомодульная система счисления использует взаимно простые позиционные основания, которые будучи определённым образом упорядочены образуют **вектор оснований**. Остатки, формируемые при представлении целого числа в многомодульной АВ и упорядоченные в соответствии со структурой вектора оснований, называются **стандартным набором остатков** относительно данного вектора оснований. Замечание. В многомодульной АВ ( по аналогии с одномодульной АВ ) мы можем для данного вектора оснований определить : ибо наименьшую неотрицательную числовую систему; либо (если все модули нечётные) наименьшую по абсолютной величине числовую систему или симметричную систему остатков.

**Изоморфизм модульных арифметик**

Рассмотрим вектор оснований: β = [ m 1 , m 2 , … , m n ] , ( m i , m j ) = 1 для i ≠ j Пусть M = m1 \* m2 \*…\* mn (Т.к. модули попарно взаимно просты, то M их НОК).

Теорема. Два целых числа n 1 и n 2 имеют одинаковые стандартные наборы остатков относительно вектора оснований β = [ m 1 , m 2 , … , m n ], тогда и только тогда, когда n 1 ≡ n 2 ( mod m 1 \* m 2 \* … \* m n ).

Из теоремы следует, что множество Z β = { n ( mod β ) : n ∈ Z } содержит M элементов, которые взаимно однозначно отображаются на элементы множества ZM.

Нетрудно показать,что два множества Z β и Z M с соответ.-ми операциями сложения и умножения представляют собой **изоморфные** конечные коммутативные кольца, т.е. многомодульная арифметика эквивалентна арифметике по модулю M .

**Многомодульная АВ – реализация**

Важное преимущество многомодульной числовой системы состоит в отсутствии переносов при выполнении операций сложения и умножения. Арифметика замкнута в каждой позиции (т.е. арифметические действия выполняются полностью и независимо в разных позициях). Поэтому можно выполнять сложение и умножение длинных целых чисел так же быстро, как и обычных (коротких) целых чисел. При реализации многомодульной АВ на двоичных компьютерах удобно использовать модули следующего вида : m = 2e – 1, т.е. каждый модуль на единицу меньше, чем степень двойки. В некоторых случаях необходимо знать, являются ли модули взаимно простыми. Если они имеют вид 2e –1, то для проверки этого можно использовать следующее правило : ( 2 e –1, 2 f –1)= 2 ( e , f ) – 1. Из указанного правила следует, что модули взаимно просты тогда и только тогда, когда числа e и f взаимно просты.

Замечание. Правило следует из алгоритма Евклида и следующего тождества : ( 2 e – 1 )( mod (2 f – 1) ) = 2 e ( mod f ) – 1.

**Операция деления**

Для выполнения операции деления в многомодульной АВ определим элемент b – 1 ( mod β ) мультипликативно обратный к элементу b = [ b 1 , b 2 , … , b n ] по модулю вектора оснований β = [ m 1 , m 2 , … , m n ] следующим образом : b – 1 (mod β) = [ ( b1 ) – 1 (mod m1) , ( b2 ) – 1 (mod m2) , … , ( bn ) – 1 ( mod m n ) ]

Далее, если a = [ a 1 , a 2 , … , a n ] , то :

a / b ( mod β ) = [ a 1 \* ( b 1 ) – 1 ( mod m 1 ) ,

a 2 \* ( b 2 ) – 1 ( mod m 2 ) ,

. . . . . . . . . . . . . . . . . . . . .

a n \* ( b n ) – 1 ( mod m n ) ].

**Сравнение чисел**

Замечание. Используя симметричную систему остатков, можно вычесть из одного числа другое и затем определить знак разности. Но остатки в симметричной системе не несут информации о знаке числа, поэтому для определения знака потребуется преобразование к обычному (не модульному) виду, что означает отказ от многомодульной АВ.

Задача определения знака числа может быть эффективно решена с помощью преобразования числа x к представлению со смешанными основаниями.

Замечание. Представление со смешанными основаниями ранее было рассмотрено при выражении решения x в греко-китайском алгоритме :

x = q 1 + q 2 \* m 1 + q 3 \* m 1 \* m 2 + … + q n \* m 1 \* m 2 \* … \* m n – 1 (\*)

где каждое q i не превосходит модуля m i , qn называется старшим членом числа x , знак числа x совпадает со знаком его старшего члена.

**Знак числа**

Замечание. Для определения знака числа удобно, чтобы последний модуль векторе оснований был равен 2 ,т.к. необходимо знать, в какой половине множества возможных чисел располагается результат. Пусть дано представление : x = [ a 1 , a 2 , … , a n ] относительно вектора оснований : β = [ m 1 , m 2 , … , m n ].

Как вычислить знак числа x ? Для определения знака числа x необходимо преобразовать это число к форме со смешанными основаниями и определить знак старшего члена. Для этого необходимо вычислить цифры q 1 , q 2 , … , q n. Очевидно, что из формулы (\*) следует : x ≡ q 1 ( mod m 1 ) , т.е. q 1 = a 1 (тем самым получена 1-я цифра).

Вычислим разность x – q1(вычитая q1 из каждого остатка, представляющего x). Имеем : x – q1 = q2 \* m1 + q3 \* m1 \* m2 + … + qn \* m1 \* m2 \* … \* mn–1 . Первая цифра (в смешанном представлении) числа x – q 1 равна нулю, поэтому первые цифры всех последующих чисел можно будет не рассматривать.

Таким образом, будем считать, что размерность вектора x – q 1 равна n–1. Теперь найдём ( m 1 ) – 1 ( mod β r ) (многомодульный) мультипликативный обратный к элементу m1 по модулю β r элемент , где β r = [m2 , … , 2] (имеет размерность n–1).

Далее вычислим (многомодульное) произведение ( x – q 1 ) \* ( m 1 ) – 1 чтобы получить вторую цифру q 2 .

Будем продолжать этот процесс, пока не вычислим q n . При q n = 0 x > 0 , при q n = 1 x < 0.