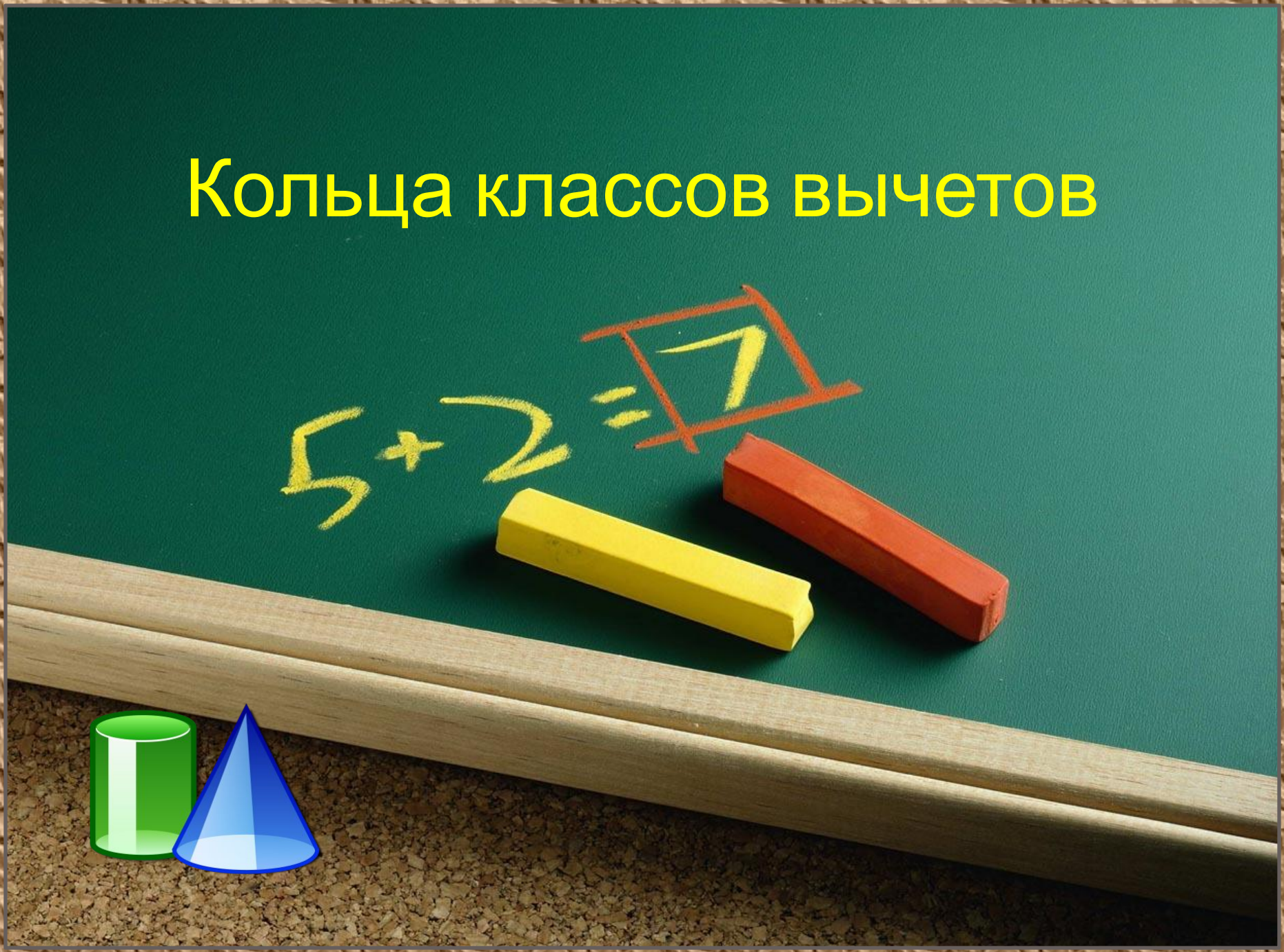
Кольца классов вычетов



Кольцо Zm классов вычетов по модулю m

- Классом вычетов по модулю m с представителем $a \in Z$ называется множество $[a] = \{x \in Z : x \equiv a \pmod m\}$.
- Определение 1. Суммой классов вычетов [a] и [b] называется класс вычетов, содержащий число a + b: [a] + [b] = [a + b].
- Определение 2. Произведением классов вычетов [a] и [b] называется класс вычетов, содержащий число ab: [a] · [b] = [ab].
- Теорема 1. Сумма и произведение классов вычетов, определенные выше, не зависят от выбора представителей классов. ДОКАЗАТЕЛЬСТВО. Пусть [a1] = [a] и [b1] = [b]. Тогда $a1 \equiv a \pmod m$, $b1 \equiv b \pmod m$. Используя свойства сравнений (см. § 1 раздела II), находим $a1 + b1 \equiv a + b \pmod m$, $a1b1 \equiv ab \pmod m$. Следовательно, [a1 + b1] = [a + b] и [a1b1] = [ab]. в, содержащий число ab: [a] · [b] = [ab].

Кольцо Zm классов вычетов по модулю m

- Теорема 2. Множество Zm классов вычетов по модулю m с операциями сложения и умножения образует коммутативное кольцо с единицей.
  ДОКАЗАТЕЛЬСТВО. Убедимся, что условия, определяющие коммутативное кольцо с единицей, выполнены в случае Zm.
  1. Ассоциативность сложения. ([a] + [b]) + [c] = [a + b] + [c] = [(a + b) + c] = [a + (b + c)] = [a] + [b + c] = [a] + ([b] + [c]). Третье равенство в этой цепочке вытекает из свойства ассоциативности сложения целых чисел.
  2. Коммутативность сложения. [a] + [b] = [a + b] = [b + a] = [b] + [a]. Здесь мы воспользовались коммутативностью сложения целых чисел.
  3. Существование нулевого элемента. Нулевым элементом является класс [0], состоящий из чисел, остаток от деления которых на m равен нулю, т. е. из чисел, кратных m. Действительно, [a] + [0] = [a + 0] = [a].
  4. Существование противоположного элемента. Для класса [a] противоположным является класс [−a], содержащий число −a. В самом деле, [a] + [−a] = [a + (−a)] = [0].

Кольцо Zm классов вычетов по модулю m

- 5. Ассоциативность умножения. $([a] \cdot [b]) \cdot [c] = [ab] \cdot [c] = [(ab)c] = [a(bc)] = [a] \cdot [bc] = [a] \cdot ([b] \cdot [c])$.
  6. Коммутативность умножения. $[a] \cdot [b] = [ab] = [ba] = [b] \cdot [a]$.
  7. Дистрибутивность умножения по сложению. $([a] + [b]) \cdot [c] = [a + b] \cdot [c] = [(a + b)c] = [ac + bc] = = [ac] + [bc] = [a] \cdot [c] + [b] \cdot [c]$. При проверке условий 5—7 мы использовали свойства ассоциативности, коммутативности и дистрибутивности умножения целых чисел.
  8. Существование единичного элемента. Роль единичного элемента выполняет класс $[1]$, так как $[a] \cdot [1] = [a \cdot 1] = [a]$. Итак, проверена выполнимость всех условий, определяющих коммутативное кольцо с единицей.
- Кольцо Z_m называется кольцом классов вычетов по модулю m. Выполнение условий 1—4 означает, что относительно операции сложения множество Z_m образует абелеву группу — она называется аддитивной группой кольца Z_m. В частности, мы можем стандартным образом определить операцию вычитания классов: $[a] - [b] = [a] + [-b]$.

Группа обратимых элементов кольца Zm

- Под делением классов вычетов [b], [a] ∈ Zm мы понимаем нахождение такого класса [c] ∈ Zm (частного от деления данных классов), что [b] = [c] · [a].
- Определение 6. Если для данного класса [a] ∈ Zm существует такой класс [x] ∈ Zm, что [a] · [x] = [1] (1) ,то он называется обратным к [a]. Сам же класс [a] в этом случае называется обратимым. Обозначение: [x] = [a]^−1 .
- Теорема 4. Если класс вычетов [a] ∈ Zm взаимно прост с модулем, то он обратим. ДОКАЗАТЕЛЬСТВО. Равенство (1) равносильно сравнению ax ≡ 1 (mod m). Поскольку НОД (a, m) = 1, по теореме 7 это сравнение однозначно разрешимо. Его единственное решение [r0] и есть искомый обратный класс: [a]^−1 = [r0].
- Таким образом, класс вычетов [a] ∈ Zm обратим тогда и только тогда, когда этот класс взаимно прост с модулем m. Напомним, что таких классов всего имеется ϕ (m) штук, где ϕ(m) — функция Эйлера, а их множество обозначается Z*m

- Теорема 5. В кольце Zm возможно, и притом единственным образом, деление на любой класс [a] ∈ Z* m. Частное от деления класса [b] на [a] определяется по формуле [c] = [b] · [a]^−1 .

Поле Zp классов вычетов по простому модулю p

- Определение 7. Коммутативное кольцо с единицей, отличной от нуля, в котором каждый ненулевой элемент обратим по умножению, называется полем.
- Теорема 6. Кольцо Zm является полем тогда и только тогда, когда m = p — простое число.
  ДОКАЗАТЕЛЬСТВО. Как известно, в поле отсутствуют делители нуля, поэтому если m — составное число, то Zm — не поле. С другой стороны, если m = p — простое число, то, как уже отмечалось, группа обратимых элементов Z* p состоит из всех ненулевых классов вычетов. Следовательно, Zp — поле.
- Как и над всяким полем, над полем Zp можно рассматривать многочлены. Некоторые из доказанных нами ранее фактов превращаются в частные случаи общих теорем теории многочленов.

Поле Zp классов вычетов по простому модулю p

- В заключение обратим внимание на одну особенность алгебры многочленов над полем Zp: если f(x) — произвольный многочлен с коэффициентами из Zp, то справедливо тождество f(x)^p = f(x^p).

Порядок класса вычетов

- Теорема 7. Если [a] ∈ Z*m — обратимый класс вычетов, то [a]^(ϕ(m)) = [1].
- Определение 8. Порядком класса вычетов [a] ∈ Z*m называется наименьшее натуральное число δ такое, что [a]^δ = [1]. То, что такое число δ существует, вытекает, например, из теоремы 7, которая даже гарантирует неравенство δ≤ϕ(m).
- Определение 8 можно сформулировать в следующих терминах. Пусть НОД (a, m) = 1. Порядком числа a по модулю m называется наименьшее натуральное число δ такое, что a^δ ≡ 1 (mod m). Говорят также, что число a принадлежит показателю δ по модулю m. Ясно, что для всех чисел из [a] показатель δ, которому они принадлежат, один и тот же.
- Теорема 8. Пусть δ — порядок класса вычетов [a] ∈ Z*m. Равенство [a]^k = [1] имеет место тогда и только тогда, когда k ≡ 0 (mod δ).

Первообразные корни

- Определение 9. Пусть НОД (g, m) = 1. Если порядок класса вычетов [g] ∈ Z*m равен ϕ(m), то число g называется первообразным корнем по модулю m.
- С теоретико-групповой точки зрения вопрос о наличии первообразных корней по модулю m — это вопрос о том, будет ли группа Z*m циклической, т. е. будет ли она состоять из целых степеней какого-нибудь одного класса вычетов. Следующая теорема впервые была доказана Гауссом.
- Теорема 9. Если модуль m есть простое число p, то первообразные корни существуют.