МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения
высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«___» _____ 2019 г.

АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ

Методические указания к лабораторным занятиям для студентов направления подготовки бакалавриата 02.03.03«Математическое обеспечение и администрирование информационных систем»

Курск 2019

УДК 512 (075.8)
Составитель: В.П. Добрица

Рецензент
Кандидат технических наук, доцент кафедры «Информационные системы и технологии» Ю.А. Халин

Алгебра и теория чисел: методические указания к лабораторным занятиям / Юго-Зап. гос. ун-т; сост.: В.П. Добрица. – Курск, 2019. – 28 с.: табл. 5. – Библиогр.: с. 28.

В методических указания описываются основные алгебры и теории чисел. Изложены краткие теоретические сведения, приведены примеры решения задач, а также задачи для самостоятельного решения.

Методические рекомендации предназначены для студентов, обучающихся по направлению 02.03.03 «Математическое обеспечение и администрирование информационных систем».

Текст печатается в авторской редакции

Подписано в печать . Формат 60х84 1/16.
Усл.печ. л. 1,34. Уч.-изд. л. 1,21. Тираж 100 экз.
Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

СОДЕРЖАНИЕ 3
Сравнение по модулю 4
Системы вычетов 12
Сравнение первой степени 22
ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ ПО ДИСЦИПЛИНЕ «АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ» 26
Список литературы 28

ЛАБОРАТОРНОЕ ЗАНЯТИЕ №1

Сравнение по модулю

Вопросы к занятию:

1. Определение и свойства сравнений
2. Арифметические приложения сравнений

Краткие сведения из теории

Два целых числа *a и b сравнимы по модулю m*, если при делении на *m* они дают одинаковые остатки. Число *m* называется модулем сравнения.

Эквивалентная формулировка: *a и b* сравнимы по модулю *m*, если их разность *a – b* делится на *m* без остатка, или если *a* может быть представлено в виде $a = b + k \cdot m$, где *k* - некоторое целое число.

Например: 32 и – 10 сравнимы по модулю 7, так как

$32 = 7 \cdot 4 + 4$ и $-10 = 7 \cdot (-2) + 4$,

11 и 21 сравнимы по модулю 10, т.к. $(11 - 21) \vdots 10$,

$2 \equiv 10 \pmod 8$ т.к. $(2 - 10) \vdots 8$

$35 \equiv 27 \pmod 8$ т.к. $35 = 27 + 8 \cdot 1$.

Утверждение « *a и b* сравнимы по модулю *m*» записывается в виде: $a \equiv b \pmod m$.

Свойства сравнений. Отношение сравнимости по модулю натурального числа обладает следующими свойствами:

- рефлексивности: для любого целого *a* справедливо $a \equiv a \pmod m$.
- симметричности: если $a \equiv b \pmod m$, *то* $b \equiv a \pmod m$.
- транзитивности:

если $a \equiv b \pmod m$ и $b \equiv c \pmod m$, *то* $a \equiv c \pmod m$.

В силу этих трех свойств отношение сравнимости является отношением эквивалентности на множестве целых чисел.

Любые два целых числа сравнимы по модулю 1.

Если числа**: *a и b*** сравнимы по модулю ***m,*** то есть $a \equiv b \pmod m$ и ***m*** делится на ***n,*** то ***a*** и ***b*** сравнимы по модулю ***n,***то есть $a \equiv b \pmod n$.

Для того чтобы два числа ***a и b*** были сравнимы по модулю ***m***, каноническое разложение на простые множители которого:

$m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_i}$, $i=1,2,\ldots,d$ необходимо и достаточно, чтобы

$a \equiv b \pmod{p^{\alpha_i}}$, $i=1,2,\ldots,d$.

Если $a \equiv b \pmod{m_1}$ и $a \equiv b \pmod{m_2}$, то $a \equiv b \pmod m$,

где $m = [m_1, m_2]$.

Сравнения по одному и тому же модулю обладают многими свойствами обычных равенств. Например, их можно складывать, вычитать и перемножать:

если числа $a_1, a_2,\ldots,a_n$ и $b_1,b_2,\ldots,b_n$ попарно сравнимы по модулю ***m***, Место для формулы.то и их суммы $(a_1+ a_2+\ldots+a_n)$ и $(b_1+b_2+\ldots+b_n)$ и произведения $(a_1 \cdot a_2 \cdot \ldots \cdot a_n)$ и $(b_1 \cdot b_2 \cdot \ldots \cdot b_n)$ также сравнимы по модулю ***m***.

Если числа ***a и b*** сравнимы по модулю ***m,*** то и их степени a^k и b^k также сравнимы по модулю ***m*** при любом натуральном ***k***.

Пример. Используя это свойство можно находить остатки от деления чисел.

Пусть необходимо найти остаток от деления $\mathbf{1234^{2327}}$ **на 11.**

Решение. $1234^{2327} \equiv r \pmod{11}$. $1234 = 11 \cdot 112 + 2 \rightarrow 1234 \equiv 2 \pmod{11}$, тогда по свойству получим $1234^{2327} \equiv 2^{2327} \pmod{11}$.

Мы знаем степени числа 2, например $2^{10} = 1024$, но $1024 = 11 \cdot 93 + 1$, тогда

$2^{10} \equiv 1 \pmod{11} \rightarrow (2^{10})^{232} \equiv 1^{232} \pmod{11} \rightarrow 2^{2320} \equiv 1 \pmod{11}$.

Теперь рассмотрим $2^7 = 128 = 11 \cdot 11 + 7$, откуда $2^7 \equiv 7 \pmod{11}$.

Получили $2^{2320} \equiv 1 \pmod{11}$ и $2^7 \equiv 7 \pmod{11}$. По свойству произведения сравнений одного модуля получим:

$\cdot\ 2^7 \equiv$

2^{2320} $1 \cdot 7 \pmod{11} \rightarrow 2^{2327} \equiv 7 \pmod{11}$.

Используя свойство транзитивности, получим

$1234^{2327} \equiv 2^{2327} (mod\ 11)$ и $\rightarrow$ $1234^{2327} \equiv 7 (mod\ 11)$,

То есть остаток от деления 1234^{2327} на 11 равен 7.

Однако нельзя сравнения делить друг на друга или на другие числа. Так, если $14 \equiv 20 (\mathrm{mod}\ 6)$, то сократив на 2, мы получим ошибочное сравнение $7 \equiv 10 (\mathrm{mod}\ 6)$ т.к. (7 – 10) не делится на 6 без остатка; или $24 \equiv 4 (\mathrm{mod}\ 10) \rightarrow 6 \cdot 4 \equiv 1 \cdot 4 (\mathrm{mod}\ 10)$, но сравнение $6 \equiv 1 (\mathrm{mod}\ 10)$ неверно.

Правила сокращения для сравнений следующие:

- Можно делить обе части сравнения на число, взаимно простое с модулем, если $ac \equiv bc (\mathrm{mod}\ m)$ и $(c;m) = 1$, то $a \equiv b (\mathrm{mod}\ m)$.

- Можно одновременно разделить обе части сравнения и модуль на их общий делитель: если $ac \equiv bc (\mathrm{mod}\ mc)$, то $a \equiv b (\mathrm{mod}\ m)$.

Нельзя также выполнять указанные операции, если модули не совпадают.

Классы вычетов. Множество всех чисел, сравнимых с a по модулю m, называется классом вычетов по модулю m и обозначается $\overline{a}$.

Таким образом, сравнение $a \equiv b (\mathrm{mod}\ m)$ равносильно $\overline{a_m} = \overline{b_m}$.

Системы вычетов. Система вычетов позволяет осуществлять арифметические операции над конечным набором чисел, не выходя за его пределы. ***Полная система вычетов по модулю m*** – любой набор из m попарно несравнимых по модулю m целых чисел. Обычно в качестве полной системы вычетов по модулю m берутся наименьшие неотрицательные вычеты 0, 1, …. m – 1, или абсолютно наименьшие вычеты, состоящие

из чисел $0, \pm 1, \pm 2, \ldots \pm \frac{m-1}{2}$ в случае нечетного m,

и чисел $0, \pm 1, \pm 2, \ldots \pm (m/2 - 1), \frac{m}{2}$ в случае четного m.

Максимальный набор попарно несравнимых по модулю m чисел, взаимно простых с m, называется **приведенной системой вычетов** по модулю m.

Всякая приведенная система вычетов по модулю m содержит

$$\varphi(m)$$

$\varphi(m)$ элементов, здесь - функция Эйлера.

Теорема Эйлера. Для любых взаимно простых чисел имеет место формула $a^{\varphi(m)} \equiv 1(mod\ m)$

Теорема Ферма. Если p - простое число и p не делит a , то

$$a^p \equiv a(mod\ p)$$

Указанные теоремы также используются для нахождения остатков от деления различных чисел. [Файл mht:Лекции по теории чисел, мои документы]

Пример 1. Девятая степень однозначного числа оканчивается на 7. Найти это число.

Решение. а ^{9} □□7(mod 10) – это дано. Кроме того, очевидно, что (7, 10)=1 и (a , 10)=1. По теореме Эйлера, а □□(10) □□1(mod 10). Следовательно, а ^{4} □□1(mod 10) и, после возведения в квадрат, а ^{8} □□1(mod 10). Поделим почленно а ^{9} □□7(mod 10) на а ^{8} □□1(mod 10) и получим а □□7(mod 10). Это означает, что а=7.

Пример 2. Доказать, что 1 ^{18} +2 ^{18} +3 ^{18} +4 ^{18} +5 ^{18} +6 ^{18} □□-1(mod 7)

Доказательство. Числа 1, 2, 3, 4, 5, 6 взаимно просты с 7. По теореме Ферма имеем:

$$\begin{cases} 1^6 \equiv 1(\mathrm{mod}\ 7) \\ 2^6 \equiv 1(\mathrm{mod}\ 7) \\ \quad\vdots \\ 6^6 \equiv 1(\mathrm{mod}\ 7) \end{cases}$$

Возведем эти сравнения в куб и сложим:

1 ^{18} +2 ^{18} +3 ^{18} +4 ^{18} +5 ^{18} +6 ^{18} □□6(mod 7) □□-1(mod 7)

Пример 3. Найти остаток от деления 7^{402} на 101 .

Решение. Число 101 – простое, (7, 101)=1, следовательно, по теореме Ферма: $7^{100} \equiv 1 \pmod{101}$. Возведем это сравнение в четвертую степень: $7^{400} \equiv 1 \pmod{101}$, домножим его на очевидное сравнение $7^{2} \equiv 49 \pmod{101}$, получим: $7^{402} \equiv 49 \pmod{101}$. Значит, остаток от деления 7^{402} на 101 равен 49.

Пример 4. Найти две последние цифры числа 243^{402}.

Решение. Две последние цифры этого числа суть остаток от деления его на 100. Имеем: 243=200+43; $200+43 \equiv 43 \pmod{100}$ и, возведя последнее очевидное сравнение в 402-ую степень, раскроем его левую часть по биному Ньютона (мысленно, конечно). В этом гигантском выражении все слагаемые, кроме последнего, содержат степень числа 200, т.е. делятся на 100, поэтому их можно выкинуть из сравнения, после чего понятно, почему $243^{402} \equiv 43^{402} \pmod{100}$. Далее, 43 и 100 взаимно просты, значит, по теореме Эйлера, $43^{\varphi(100)} \equiv 1 \pmod{100}$. Считаем:

$$\varphi(100)=\varphi(2^{2}\cdot 5^{2})=(10-5)(10-2)=40.$$

Имеем сравнение: $43^{40} \equiv 1 \pmod{100}$, которое немедленно возведем в десятую степень и умножим почленно на очевидное сравнение, проверенное на калькуляторе: $43^{2} \equiv 49 \pmod{100}$. Получим:

$$\times\begin{cases} 43^{400} \equiv 1 \pmod{100} \\ 43^{2} \equiv 49 \pmod{100} \end{cases}$$

$$43^{402} \equiv 49 \pmod{100},$$

следовательно, две последние цифры числа 243^{402} суть 4 и 9 .

Пример 5. Доказать, что $(73^{12}-1)$ делится на 105.

Решение. Имеем: $105=3\cdot 5\cdot 7$, (73,3)=(73,5)=(73,7)=1. По теореме Ферма:

$$73^{2} \equiv 1 \pmod 3$$

$$73^{4} \equiv 1 \pmod 5$$

$$73^{6} \equiv 1 \pmod 7$$

Перемножая, получаем:

$$73^{12} \equiv 1 \pmod 3, \pmod 5, \pmod 7,$$

откуда, по свойствам сравнений, изложенным в пункте 16, немедленно следует:

$$73^{12} - 1 \equiv 0 \pmod{105},$$

ибо 105 - наименьшее общее кратное чисел 3, 5 и 7 . Именно это и требовалось.

Пример. Необходимо найти остаток от деления числа 12^{2751} на 5.

Решение. $12^{2751} \equiv r \pmod 5$. (12; 5) = 1; след. 12 и 5 взаимно простые числа, по теореме Эйлера $12^{\varphi(5)} \equiv 1 \pmod 5$; $\varphi(5) = 4 \rightarrow 12^{4} \equiv 1 \pmod 5$;

Но $2751 = 4 \cdot 687 + 3$;

тогда $(12^{4})^{687} \equiv 1^{687} \pmod 5 \rightarrow$ **$12^{2748} \equiv 1 \pmod 5$** и $12 \equiv 2 \pmod 5 \rightarrow$ **$12^{3} \equiv 2^{3} \pmod 5$**

Но $8 \equiv 3 \pmod 5$, здесь **используем свойство транзитивности, по которому Если $12^{3} \equiv 2^{3} \pmod 5$ и $8 \equiv 3 \pmod 5$, то $12^{3} \equiv 3 \pmod 5$.**

А теперь перемножим $12^{2748} \cdot 12^{3} \equiv 1 \cdot 3 \pmod 5 \rightarrow 12^{2751} \equiv 3 \pmod 5$.

Таким образом, остаток от деления числа 12^{2751} на 5 равен 3.

КОНТРОЛЬНОЕ ЗАДАНИЕ

Задание 1. Какие из следующих сравнений являются верными:

Вариант 1. $1 \equiv -5 \pmod 6$; Вариант 2. $546 \equiv 0 \pmod{13}$;

Вариант 3. $21 \equiv 1 \pmod 4$; Вариант 4. $121347 \equiv 92817 \pmod{10}$;

Вариант 5. $31 \equiv -9 \pmod{10}$; Вариант 6. $35 \equiv 27 \pmod 8$;

Вариант 7. $99 \equiv 11 \pmod 4$; Вариант 8. $1347 \equiv 817 \pmod{10}$;

Вариант 9. $10 \equiv -14 (\mathrm{mod}\ 6)$; Вариант 10. 546 □ 0(mod 13);

Вариант 11. 23 □ -1 (mod 4); Вариант 12. $347 \equiv 817 (\mathrm{mod}\ 10)$;

Вариант 13. $1 \equiv -5 (\mathrm{mod}\ 6)$; Вариант 14. 546 □ 0(mod 13);

Вариант 15. 16385 □ 1(mod 4); Вариант 16.$121347 \equiv 92817 (\mathrm{mod}\ 10)$;

Вариант 17. $1331 \equiv 0 (\mathrm{mod}\ 11)$; Вариант 18. 28561 □ 0(mod 13);

Вариант 19. 16808 □ 1 (mod 7); Вариант 20. $121347 \equiv 92817 (\mathrm{mod}\ 10)$;

Вариант 21. $7775 \equiv -1 (\mathrm{mod}\ 6)$; Вариант 22. 2197 □ 0(mod 13);

Задание 3. Найти две последние цифры числа a^n:

Вариант 1. 9^{10} ; Вариант 2. 9^9; Вариант 3. 6^{32}; Вариант 4. 8^{18} ;

Вариант 5. 4^{20} ; Вариант 6. 2^{100}; Вариант 7. 19^{321}; Вариант 8. 131^{161} ;

Вариант 9. 243^{402} ; Вариант 10. 17^{61}; Вариант 11. 19^{79};

Вариант 12. 7^{114} ; Вариант 13. 11^{203} ; Вариант 14. 7^{302}; Вариант 15. 6^{32};

Вариант 16. 8^{18} ; Вариант 17. 11^{203} ; Вариант 18. 19^{82} ; Вариант 19. 2^{54} ;

Вариант 20. 11^{203} ; Вариант 21. 7^{302}; Вариант 22. 6^{32}.

Задание 4. Найти остаток от деления числа a^n на m:

Вариант 1. 20^{11} , m=9; Вариант 2. 383^{175}, m=45; Вариант 3. 109^{345}, m=14;

Вариант 4. 439^{291} , m=60; Вариант 5. 293^{275} , m=48; Вариант 6. 93^{41}, m=111;

Вариант 7. 3^{80}, m=11; Вариант 8. 20^{17} , m=9; Вариант 9. 3^{200}, m=101;

Вариант 10. 11^{65}, m=80; Вариант 11. 7^{402} , m=101; Вариант 12. 13^{88}, m=89;

Вариант 13. 3^{157}, m=100; Вариант 14. 15^{231}, m=16; Вариант 15. 208^{208} , m=23;

Вариант 16. 13^{88}, m=89; Вариант 17. 11^{65}, m=80; Вариант 18. 66^{17} , m=7;

Вариант 19. 117^{53}, m=11; Вариант 20. 11^{1841}, m=7;

Задание 5. Найти остаток от деления суммы $a + b + c$ на m:

Вариант 1. $3^{80} + 7^{80}$, m=11;

Вариант 2. $3^{100} + 5^{100}$, m=7;

Вариант 3. $2^{100}+3^{100}$, m=5;

Вариант 4. $5^{70} +7^{50}$, m=12;

Вариант 5. $12^{1231} + 14^{4324}$, m=13;

Вариант 6. $7^{65} + 11^{65}$, m=80;

Вариант 7. $3^{200} + 7^{200}$, m=101;

Вариант 8. $5^{80} + 7^{100}$, m=13;

Вариант 9. $5^{70} + 7^{50}$, m=12;

Вариант 10. $13^{100} + 5^{50}$, m=18;

Вариант 11. $3^{80} + 7^{80}$, m=11;

Вариант 12. $2^{100} + 3^{100}$, m=5;

Вариант 13. $3^{80} + 7^{80}$, m=11;

Вариант 14. $3^{100} + 5^{100}$, m=7;

Вариант 15. $3^{80} + 7^{80}$, m=11;

Вариант 16. $3^{100} + 5^{100}$, m=7;

Вариант 17. $2^{100}+3^{100}$, m=5;

Вариант 18. $5^{70} +7^{50}$, m=12;

Вариант 19. $12^{1231} + 14^{4324}$, m=13;

Вариант 20. $7^{65} + 11^{65}$, m=80;

ЛАБОРАТОРНОЕ ЗАНЯТИЕ №2
Системы вычетов

Вопросы к занятию:
1. Определение и свойства вычетов
2. Классы вычетов. Системы вычетов

Краткие сведения из теории

Применяя теорему о делении с остатком можно множество целых чисел разбить на ряд классов. Рассмотрим пример. Пусть $m = 6$. Тогда имеем шесть классов разбиения множества целых чисел по модулю 6:

$K_0 = \{\ldots,-18,-12,-6,0,6,6,12,18,\ldots\}$, $r = 0$;

$K_1 = \{\ldots,-17,-11,-5,1,7,13,19,\ldots\}$, $r = 1$;

$K_2 = \{\ldots,-16,-10,-4,2,8,14,20,\ldots\}$, $r = 2$;

$K_3 = \{\ldots,-15,-9,-3,3,9,15,21,\ldots\}$, $r = 3$;

$K_4 = \{\ldots,-14,-8,-2,4,10,16,22,\ldots\}$, $r = 4$;

$K_5 = \{\ldots,-13,-7,-1,5,11,17,23,\ldots\}$, $r = 5$;

где через r обозначен остаток от деления целого числа на 6.

Напомним теорему о делении с остатком:

Теорема: Разделить число $a \in Z$ на число $b \in Z$, $b \neq 0$, с остатком, значит, найти пару целых чисел q и r, таких, что выполняются следующие условия:

$a = bq + r, 0 \leq r < |b|$.

Легко доказывается, что для любых целых чисел a и $b \neq 0$ деление с остатком возможно и числа q и r определяются однозначно. В нашем примере полная система наименьших неотрицательных вычетов есть множество {0, 1, 2, 3, 4, 5}; полная система наименьших положительных вычетов – множество {0, 1, 2, 3, 4, 5}; полная система наименьших по абсолютной величине вычетов – множество {-2,-1, 0, 1, 2, 3}; приведённая система вычетов – множество {1,5}, так как $\varphi(6) = 6(1 - 1/2)(1 - 1/3) = 2$; фактор-множество $Z/\equiv_6 = \{K_0, K_1, K_2, K_3, K_4, K_5\}$.

Один из методов выполнения арифметических операций над данными целыми числами основан на простых положениях теории чисел. Идея этого метода состоит в том, что целые числа представляются в одной из непозиционных систем – в системе остаточных классов. А именно: вместо операций над целыми числами оперируют с остатками от деления этих чисел на заранее выбранные простые числа – модули $p_1, p_2, \ldots, p_n$.

Чаще всего числа $p_1, p_2, \ldots, p_n$ выбирают из множества простых чисел.

Пусть $A \equiv a_1 (\mathrm{mod}\, p_1), A \equiv a_2 (\mathrm{mod}\, p_2), \ldots, A \equiv a_n (\mathrm{mod}\, p_n)$.

Так как в кольце целых чисел имеет место теорема о делении с остатком, т. е. $\forall a \in Z \forall b \in Z b \neq 0 \exists q \in Z \exists r \in Z,$ где $r \geq 0, a = bq + r, r < |b|$, то кольцо Z, по определению, является евклидовым.

Таким образом, в качестве чисел $a_i (i = \overline{1,n})$ можно выбрать остатки от деления числа A на p_i соответственно.

Система вычетов позволяет осуществлять арифметические операции над конечным набором чисел, не выходя за его пределы. **Полная система вычетов** по модулю n — любой набор из n попарно несравнимых по модулю n целых

чисел. Обычно в качестве полной системы вычетов по модулю n берутся наименьшие неотрицательные вычеты

Делении целых чисел ***a*** и ***m*** получается частное ***q*** и остаток ***r***, такие что

$a = m \cdot q + r,\ 0 \le r \le m-1$. Остаток ***r*** называют **ВЫЧЕТ**ом по модулю **m**.

Например, для $m = 3$ и для $m = 5$ получим:

$a = m \cdot q + r,\ m = 3$	$a = m \cdot q + r,\ m = 5$
$0 = 3 \times 0 + 0$	$0 = 5 \times 0 + 0$
$1 = 3 \times 0 + 1$	$1 = 5 \times 0 + 1$
$2 = 3 \times 0 + 2$	$2 = 5 \times 0 + 2$
$3 = 3 \times 1 + 0$	$3 = 5 \times 0 + 3$
$4 = 3 \times 1 + 1$	$4 = 5 \times 0 + 4$
$5 = 3 \times 1 + 2$	$5 = 5 \times 1 + 0$
$6 = 3 \times 2 + 0$	$6 = 5 \times 1 + 1$
$7 = 3 \times 2 + 1$	$7 = 5 \times 1 + 2$

Если остаток равен нулю (***r*=0**), то говорят, что **m** делит ***a*** нацело (или **m** кратно ***a***), что обозначают $m \vdots a$, а числа ***q*** и ***m*** называют делителями ***a***. Очевидно $1 \vdots a$ и $a \vdots a$. Если ***a*** не имеет других делителей, кроме ***1*** и ***a***, то ***a*** – простое число, иначе ***a*** называют составным числом. Самый большой положительный делитель ***d*** двух чисел ***a*** и ***m*** называют наибольшим общим

делителем (НОД) и обозначают ***d = (a,m).*** Если НОД ***(a,m)= 1***, то ***a*** и ***m*** не имеют общих делителей, кроме ***1***, и называются взаимно простыми относительно друг друга.

Каждому **ВЫЧЕТу** ***r = 0, 1, 2,…, m-1*** соответствует множество целых чисел ***a, b, …*** Говорят, что числа с одинаковым **ВЫЧЕТ**ом сравнимы по модулю и обозначают $a \equiv b(\mathrm{mod}\ m)$ или $(a \equiv b)_m$.

Например, при ***m = 3***:

r = 0 сравнимы по модулю 3 числа ….-9, -6, -3, 0, 3, 6, 9,….
r = 1 сравнимы по модулю 3 числа ….-8, -5, -2, 1, 4, 7, 10,….
r = 2 сравнимы по модулю 3 числа ….-7, -3, -1, 2, 5, 8, 11,….
r = 0 сравнимы по модулю 3 числа ….-9, -6, -3, 0, 3, 6, 9,….

Например, при ***m = 5***:

r = 0 сравнимы по модулю 5 числа ….-15, -10, -5, 0, 5, 10, 15,….
r = 1 сравнимы по модулю 5 числа ….-14, -9, -4, 1, 6, 11, 16,….
r = 2 сравнимы по модулю 5 числа ….-13, -8, -3, 2, 7, 12, 17,….
r = 3 сравнимы по модулю 5 числа ….-12, -7, -2, 3, 8, 13, 18,….
r = 4 сравнимы по модулю 5 числа ….-11, -6, -1, 4, 9, 14, 19,….

Числа ***a***, которые сравнимы по модулю ***m*** , образуют класс своего **ВЫЧЕТа** ***r*** и определяются как ***a = m· q + r.***

Числа ***a*** тоже называют **ВЫЧЕТами** по модулю ***m***. Неотрицательные **ВЫЧЕТы *a* = *r*** (при ***q=0***), принимающие значения из интервала ***[0, 1,..m – 1]***, образуют полную систему наименьших вычетов по модулю ***m.***

ВЫЧЕТы ***a***, принимающие значения из интервала **[-(m – 1)/2) (m – 1)/2)**

(,…,( ], при **нечетном *m*** или из интервала **[-*m*/2, …, *m*/2 – 1]** , при **четном *m*** образуют полную систему абсолютно наименьших **ВЫЧЕТ**ов по модулю ***m.***

Например, при ***m*** = 5 классы наименьших вычетов образуют r = 0, 1, 2, 3, 4, a = -2, -1, 0, 1, 2. Обе приведенные совокупности чисел образуют полные системы **вычет**ов по модулю **5** .

Класс **ВЫЧЕТов**, элементы которого взаимно просты с модулем ***m***

называют приведенным. Функция Эйлера $\varphi(m)$ определяет сколько **ВЫЧЕТов** из полной системы наименьших вычетов по модулю ***m*** взаимно просты с ***m***. При простом ***m=p*** имеем $\varphi(m)$ = ***p-1.***

Определение. Максимальный набор попарно несравнимых по модулю ***m*** чисел, взаимно простых с ***m***, называется **приведённой системой вычетов** по модулю *m*. Всякая приведённая система вычетов по модулю *m* $\varphi(m)$

содержит элементов, где $\varphi(m)$ — функция Эйлера.

Определение. Любое число из класса эквивалентности ϵ_m будем называть **вычет**ом по модулю *m* . Совокупность **вычет**ов, взятых по одному из

каждого класса эквивалентности ϵ_m, называется полной системой **вычет**ов по модулю m (в полной системе **вычет**ов, таким образом, всего m штук чисел). Непосредственно сами остатки при делении на m называются наименьшими неотрицательными **вычет**ами и, конечно, образуют полную систему **вычет**ов по модулю m. **Вычет** ρ называется абсолютно наименьшим, если $|\rho|$ наименьший среди модулей **вычет**ов данного класса.

Пример. Проверить, образуют ли числа 13, 8, - 3, 10, 35, 60 полную систему вычетов по модулю m=6.

Решение: По определению числа образуют полную систему вычетов по модулю **m**, если их ровно m и они попарно несравнимы по модулю **m**.

Попарную несравнимость можно проверить, заменив каждое число наименьшим неотрицательным вычетом; если повторений не будет, то это полная система вычетов.

Применим теорему о делении с остатком: $\boldsymbol{a = m \cdot q + r.}$

$13 = 6 \cdot 2 + 1 \rightarrow 13 \equiv 1 (\mathrm{mod}\ 6)$; $8 = 6 \cdot 1 + 2 \rightarrow 8 \equiv 2 (\mathrm{mod}\ 6)$;
$-3 = 6 \cdot (-1) + 3 \rightarrow -3 \equiv 3 (\mathrm{mod}\ 6)$; $10 = 6 \cdot 1 + 4 \rightarrow 10 \equiv 4 (\mathrm{mod}\ 6)$;
$35 = 6 \cdot 5 + 5 \rightarrow 35 \equiv 5 (\mathrm{mod}\ 6)$; $60 = 6 \cdot 10 + 0 \rightarrow 60 \equiv 0 (\mathrm{mod}\ 6)$.

Получили последовательность чисел: 1, 2, 3, 4, 5, 0, их ровно 6, повторений нет и они попарно несравнимы. То есть, они образуют полную систему вычетов по модулю m = 6.

Пример. Заменить наименьшим по абсолютной величине, а также наименьшим положительным вычетом 185 по модулю 16.

Решение. Применим теорему о делении с остатком:

$185 = 16 \cdot 11 + 9 \rightarrow 185 \equiv 9 (\mathrm{mod}\ 16)$.

Пример. Проверить, образуют ли числа $(13, -13, 29, -9)$ приведенную систему вычетов по модулю m=10.

Решение: Всякая приведённая система вычетов по модулю m $\varphi(m)$ содержит элементов, где $\varphi(m)$ — функция Эйлера. В нашем случае

$\varphi(10)$=4, ибо среди натуральных чисел только 1, 3, 7, 9 взаимно просты с 10 и не превосходят его. То есть, возможно, что эти четыре числа составляют искомую систему. Проверим эти числа на их попарную несравнимость:

$13 = 10 \cdot 1 + 3; \rightarrow 13 \equiv 3(\text{mod } 10)$; $-13 = 10 \cdot (-2) + 7; \rightarrow -13 \equiv 7(\text{mod } 10)$;

$29 = 10 \cdot 2 + 9; \rightarrow 29 \equiv 9(\text{mod } 10)$; $-9 = 10 \cdot (-1) + 1; \rightarrow -9 \equiv 1(\text{mod } 10)$.

Все числа попарно несравнимы, среди них нет повторений, их ровно 4 и они не превосходят модуль. Следовательно, они образуют приведенную систему вычетов.

Пример. Проверить, образуют ли числа $(-349, -193, 231, 401)$ приведенную систему вычетов по модулю m=12.

Решение: В нашем случае $\varphi(12)$=4, ибо среди натуральных чисел только 1, 3, 7, 9 взаимно просты с 10 и не превосходят его. То есть, возможно, что эти четыре числа составляют искомую систему. Проверим эти числа на их попарную несравнимость:

$-349 = 12 \cdot (-30) + 11; \rightarrow -349 \equiv 11(\text{mod } 12)$;

$-193 = 12 \cdot (-17) + 11; \rightarrow -193 \equiv 11(\text{mod } 12)$;

$231 = 12 \cdot 19 + 3; \rightarrow 231 \equiv 3(\text{mod } 12)$;

$401 = 12 \cdot 33 + 5; \rightarrow 401 \equiv 5(\text{mod } 12)$.

Среди чисел есть повторения, имеем два сравнимых числа -349 и -193. Следовательно, числа не образуют приведенную систему вычетов.

КОНТРОЛЬНОЕ ЗАДАНИЕ

Задание 1. Заменить число a наименьшим по абсолютной величине, а также наименьшим положительным вычетом по модулю m.

Вариант 1. a = 185, m = 12; Вариант 2. a = 84, m = 9;

Вариант 3. a = 180, m = 10; Вариант 4. a = 82, m = 9;

Вариант 5. a = 85, m = 11; Вариант 6. a = 84, m = 8;

Вариант 7. a = 103, m = 87; Вариант 8. a = 84, m = 16;

Вариант 9. a = 15, m = 10; Вариант 10. a = 81, m = 9;

Вариант 11. a = 85, m = 15; Вариант 12. a = 74, m = 13;

Вариант 13. a = 185, m = 16; Вариант 14. a = 14, m = 9;

Вариант 15. a = 100, m = 11; Вариант 16. a = 484, m = 15;

Вариант 17. a = 153, m = 61; Вариант 18. a = 217, m = 19;

Вариант 19. a = 625, m = 25; Вариант 20. a = 624, m = 25;

Задание 3. Записать полную и приведенную систему наименьших неотрицательных и наименьших по абсолютной величине вычетов по модулю m.

Вариант 1. m = 12; Вариант 2. m = 9; Вариант 3. m = 10; Вариант 4. m = 13;

Вариант 1. m = 22; Вариант 2. m = 29; Вариант 3. m = 20; Вариант 4. m = 23;

Вариант 1. m = 11; Вариант 2. m = 19; Вариант 3. m = 14; Вариант 4. m = 15;

Вариант 1. m = 16; Вариант 2. m = 18; Вариант 3. m = 21; Вариант 4. m = 31;

Вариант 1. m = 25; Вариант 2. m = 17; Вариант 3. m = 30; Вариант 4. m = 33.

Задание 4. Проверить, образуют ли числа $(a_1, a_2, \ldots, a_n)$ полную систему вычетов по модулю m:

Вариант 1. (-253, - 138, 170, 393, 965, 2000, 47, 1660), m=8;

Вариант 2. (-181, - 303, 597, 242, 135, 186, -43, 32), m=8;

Вариант 3. (-40, - 45, 31, 26, - 48, - 34), m=6;

Вариант 4. (-23, - 43, -33, 36, 25, 21, 31), m=7;

Вариант 5. (- 18, - 11, -4, 15, 22, 17), m=6;

Вариант 6. (- 15, 11, 12, 18, 19), m=5;

Вариант 7. (- 17, 18, 20, - 9, 10, 23), m=6;

Вариант 8. (- 14, - 13, 16, 10, 18, 20, -16), m=7;

Вариант 9. (- 12, 13, -16, 9, 16, 23), m=6;

Вариант 10. (-21, - 13, -19, 3, 11, 19, 20), m=7;

Вариант 11. (36, 25, -23, 21, -43, -33, 31), m=7;

Вариант 12. (- 4, - 3, -1, -2, 0, 1, 2, 3, 4), m=9;

Вариант 13. (- 3, 13, 8, 10, 35, 60), m=6;

Вариант 14. (- 13, 13, -16, 9, 16, 23), m=10;

Проверить, образуют ли числа $(a_1, a_2, \ldots, a_n)$ приведенную систему вычетов по модулю m:

Вариант 15. (- 349, - 193, 231, 401), m=12;

Вариант 16. (-247, - 133, -197, 385), m=12;

Вариант 17. (13, -13, 29, -9), m=10;

Вариант 18. (-4, - 2, -1, 1, 2, 4), m=9;

Вариант 19. (13, - 13, 29, -9), m=10;

Вариант 20. (1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41), m=42;

Вариант2 1. (-253, - 138, 170, 393, 965, 2000, 47, 1660), m=8.

Задание 5. Сколько элементов входит в приведенную систему вычетов по модулю m:

Вариант 1. m = 95; Вариант 2. m = 90; Вариант 3. m = 70; Вариант 4. m = 23;

Вариант 5. m = 12; Вариант 6. m = 9; Вариант 7. m = 10; Вариант 8. m = 13;

Вариант 9. m = 22; Вариант 10. m = 19; Вариант 11. m = 17; Вариант 12. m = 23;

Вариант 13. m = 11; Вариант 14. m = 15; Вариант 15. m = 60; Вариант 16. m = 18;

Вариант 17. m = 121; Вариант 18. m = 95; Вариант 19. m = 100; Вариант 20. m = 31.

ЛАБОРАТОРНОЕ ЗАНЯТИЕ №3

Сравнение первой степени

Вопросы к занятию:

1. Определение и свойства сравнений первой степени
2. Теорема о неразрешимости сравнений
3. Методы решений сравнений первой степени

Краткие сведения из теории

Сравнения первой степени с одним неизвестным имеют вид

$ax \equiv b \pmod m$, где a, b, m - целые, $m > 0$.

Решить сравнение – значит, найти все целые значения переменной x, удовлетворяющие сравнению.

При решении сравнения $ax \equiv b \pmod m$ (1)

возможны случаи:

- если $(a, m) = 1$, то (1) имеет одно решение;
- если $(a, m) = d > 1$ и d делит b, то (1) имеет d решений;
  если $ax \equiv b \pmod m$, $a = a_1 d$, $b = b_1 d$, $m = m_1 d$ и x_0 - решение сравнения $a_1 x \equiv b_1 \pmod{m_1}$, то решения сравнения (1) имеют вид:

  $$x \equiv x_0, \quad x_0 + 2m_1, \ldots, \quad x_0 + (d - 1)m_1 \pmod m.$$

- если $(a, m) = d > 1$ и d не делит b, то (1) не имеет решений.

Методы решений сравнений первой степени с одним неизвестным:

1. Метод подбора. Если модуль невелик, то можно найти одно из решений последовательно подставляя в данное сравнение вместо x одно из значений 0, 1,…m-1 (или значения членов любой полной системы вычетов по модулю m).

Пример. Решить сравнение

Решение: В нашем случае при m=7: (0, 1, 2, 3, 4, 5, 6).

Если x = 0, то $3 \cdot 0 - 2 = -2;$ но -2 не делится на 7, след. x=0 не удовлетворяет сравнению.

Если x = 1, то $3 \cdot 1 - 2 = 1;$ но 1 не делится на 7, след. x=1 не удовлетворяет сравнению.

Если x = 2, то $3 \cdot 2 - 2 = 4;$ но 4 не делится на 7, след. x=2 не удовлетворяет сравнению.

Если x = 3, то $3 \cdot 3 - 2 = 7;$ но 7 делится на 7 ($7 \vdots 7$) след. x=3 удовлетворяет сравнению, а поэтому класс вычетов по модулю 7 является решением сравнения.

Если x = 4, то $3 \cdot 4 - 2 = 10;$ но 10 не делится на 7, след. x=4 не удовлетворяет сравнению.

Если x = 5, то $3 \cdot 5 - 2 = 13;$ но 13 не делится на 7, след. x=5 не удовлетворяет сравнению.

Если x = 6, то $3 \cdot 6 - 2 = 16;$ но 16 не делится на 7, след. x=6 не удовлетворяет сравнению.

$\bar{3}$

Таким образом, сравнение имеет одно решение , или $x \equiv 3 (mod\ 7)$.

Следует заметить, что (3; 7) = 1, то есть сравнение имеет только одно решение, а поэтому после нахождения решения x = 3 дальнейший подбор значений x является избыточным.

2. Метод конечных цепных дробей

Пример. Решить сравнение $111x \equiv 75 (mod\ 322)$.

Решение. (111, 322)=1. Включаем алгоритм Евклида:

$$322=11 \cdot 2+100$$

$$111=100 \cdot 1+11$$

$$100=11 \cdot 9+1$$

$$11=1 \cdot 11$$

(В равенствах подчеркнуты неполные частные.) Значит, $n=4$, а соответствующая цепная дробь такова: (2, 1, 9, 11)

$$\frac{m}{a} = \frac{322}{111} = 2 + \cfrac{1}{1 + \cfrac{1}{9 + \cfrac{1}{11}}}$$

Посчитаем числители подходящих дробей, составив для этого стандартную таблицу:

q_n	0	2	1	9	11
P_n	1	2	3	29	322

Числитель предпоследней подходящей дроби равен 29, следовательно, готовая формула дает ответ: $x \equiv (-1)^3 \cdot 29 \cdot 75 \equiv -2175 \equiv 79 (mod\ 322)$.

3. Метод Эйлера.

Теорема Эйлера. Пусть $m>1, (a,m)=1$ Тогда сравнение $ax \equiv b(mod\ m)$ имеет решение: $x \equiv b \cdot a^{\varphi(m)-1}$ (mod m).

Пример. Решить сравнение $7x \equiv 3(mod\ 10)$. Вычисляем:

$\varphi(10) = 4$; $x \equiv 3 \cdot 7^{4-1} (mod\ 10) \equiv 1029(mod\ 10) \equiv 9(mod\ 10)$.

КОНТРОЛЬНОЕ ЗАДАНИЕ

Задание1. Решить сравнения первой степени с одним неизвестным:

1) $29x \equiv 1 \pmod{17}$,

2) $21x+5 \equiv 0 \pmod{29}$,

3) $7x \equiv 15 \pmod{9}$,

4) $7x \equiv 9 \pmod{10}$,

5) $12x \equiv 7 \pmod{13}$,

6) $5x \equiv 3 \pmod{17}$,

7) $3x \equiv 5 \pmod{11}$,

8) $9x \equiv 2 \pmod{14}$,

9) $7x \equiv 11 \pmod{15}$,

10) $3x \equiv 4 \pmod{7}$.

2. Решить сравнения:

11) $72x \equiv 2 \pmod{10}$,

12) $8x \equiv 20 \pmod{12}$,

13) $6x \equiv 27 \pmod{12}$,

14) $10x \equiv 15 \pmod{35}$,

15) $9x \equiv 12 \pmod{21}$,

16) $28x \equiv 40 \pmod{44}$,

17) $24x \equiv 14 \pmod{26}$,

18) $21x \equiv 33 \pmod{45}$,

19) $30x \equiv 18 \pmod{102}$,

20) $21x \equiv 35 \pmod{77}$.

ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ ПО ДИСЦИПЛИНЕ «АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ»

1. Определение конечной непрерывной (цепной) дроби. Алгоритм Евклида нахождения конечной дроби.
2. Разложение рационального числа в непрерывную дробь.
3. Подходящие дроби, их свойства.
4. Свойства наилучших приближений действительных чисел.
5. Какие числа называются сравнимыми по модулю m? Какие значения может принимать модуль?
6. Как записывается сравнимость чисел a и b по модулю m?
7. В каком случае a и b называются несравнимыми по модулю m? Как это записать?
8. Приведите примеры пары чисел, сравнимых по модулю 7 и пары чисел, несравнимых по этому модулю.
9. Какое условие является необходимым и достаточным для того, чтобы два числа были сравнимы по модулю m?
10. Установите, сравнимы ли числа 726 и 162 по модулю 5, пользуясь: а) определением; б) признаком сравнимости чисел по модулю.
11. Какому равенству удовлетворяют числа a, b, сравнимые по модулю m?
12. По какому модулю сравнимы все числа между собой?
13. Сформулируйте свойства сравнений. Каждое свойство проиллюстрируйте примером.
14. В каком случае при делении обеих частей на одно и то же натуральное число модуль не изменяется? Приведите примеры.
15. Как строится класс вычетов?
16. называется представителем класса вычетов?
17. Какие числа удобно брать в качестве представителей?
18. Сколько существует различных классов вычетов по модулю m?
19. Имеется ли класс вычетов, играющий роль нейтрального элемента относительно операции умножения? Какой это класс?
20. Дайте определение полной системе вычетов по модулю m.
21. Может ли полная система вычетов по модулю m содержать:

a. два равных числа;

b. два числа, сравнимых по модулю m?

22. Перечислите свойства полной системы вычетов.

23. Дайте определение приведенной системе вычетов.

24. Можно ли получить приведенную систему вычетов из полной системы вычетов по модулю m?

25. Сколько чисел содержит приведенная система вычетов по модулю m?

26. Перечислите свойства приведенной системы вычетов.

27. На каком утверждении основана проверка арифметических действий с помощью сравнений?

28. Как проверить правильность результата деления?

29. Что называют сравнением с неизвестной величиной?

30. Дано сравнение $ax = b(\mathrm{mod}\ m)$. При каких условиях оно имеет единственное решение, не имеет решения, имеет $d>1$ решений?

31. К решению какого сравнения сводится решение сравнения $ax = b(\mathrm{mod}\ m)$, если $(a, m)=d>1$ и $b : d$?

32. Какая связь существует между решениями сравнения $ax = b(\mathrm{mod}\ m)$ и целыми решениями неопределенного уравнения $ax + my = b$?

Список литературы

1. Виноградов И.М. Элементы высшей математики. Часть третья. Основы теории чисел. Учебник для вузов. М.: Высш. шк. 1999. – с. 335 – 340.

2. Грибанов В.У. Сборник упражнений по теории чисел. – М.: Просвещение, 1964.

3. Шнеперман Л.Б. Сборник задач по алгебре и теории чисел: Учебное пособие. – СПб.: Изд. «Лань»,2008.- 224с.