Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра алгебры и дискретной математики

Г.А. СИКОРСКАЯ

Алгебра и теория чисел. Индивидуальная домашняя контрольная работа №2

Методические указания

Рекомендовано к изданию редакционно-издательским советом федерального государственного бюджетного образовательного высшего образования «Оренбургский государственный университет» для обучающихся по программам высшего образования по направлению подготовки 02.03.02 Фундаментальная информатика и информационные технологии

Оренбург
2017

УДК 512 : 511(076.5)
ББК 22.14 я 7+ 22.13 я7
С35

Рецензент – доцент, кандидат физико-математических наук
В.В. Носов

Сикорская, Г.А.
С35 Алгебра и теория чисел. Индивидуальная домашняя контрольная работа №2 : методические указания / Г.А. Сикорская; Оренбургский гос. ун-т. – Оренбург : ОГУ, 2017.

Методические указания «Алгебра и теория чисел. Индивидуальная домашняя контрольная работа №2» содержат подробное описание решений обязательных заданий индивидуальной контрольной работы по теории чисел, сопровожденное теоретическими справками, перечень всех заданий индивидуальной домашней контрольной работы (ИДКР), дополнительные задания, а также список рекомендуемой литературы.

Методические указания «Алгебра и теория чисел. Индивидуальная контрольная работа №2» предназначены для обучающихся по направлению подготовки 02.03.02 Фундаментальная информатика и информационные технологии.

УДК512 : 511(076.5)
ББК22.14 я 7+ 22.13 я7

Содержание

1 Предисловие

Индивидуальная домашняя контрольная работа №2 по дисциплине Б.1.Б.12 «Алгебра и теория чисел» предлагается студентам, изучающим курс алгебры и теории чисел во втором семестре, в соответствии с рабочей программой.

ИДКР №2 состоит из двух частей, первая из которых является наиболее простой (часть А.), вторая (часть В.) – содержит задания повышенной сложности.

Часть А.

Задания части А. составляют необходимый минимум ИДКР №2. Методические указания содержат подробное описание решений нулевого варианта части А., и, далее перечень индивидуальных заданий. Безупречное выполнение студентом заданий части А. соответствует оценке удовлетворительно.

Часть В.

Решение заданий части В. добавляет к удовлетворительной оценке один, либо два балла в зависимости от качества выполненной работы. Задания части В. не обеспечены ни разъяснением соответствующей теории, ни решением нулевого варианта. Предполагается самостоятельная работа студента, в частности, с использованием рекомендуемой литературы.

В заключение данных методических указаний предлагаются дополнительные задания, которые студент может выполнять в зависимости от своего желания. Дополнительные задания не входят в обязательную ИДКР, предоставляются студенту отдельно (по одной задаче из каждого раздела) и оцениваются отдельно.

2 Разделы дисциплины «Алгебра и теория чисел», изучаемые во 2 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			Вне ауд. ра-бота
			Л	ПЗ	ЛР	
1	Теория делимости	12	4	2	0	6
2	Важнейшие функции в теории чисел	12	4	0	0	8
3	Сравнения	16	6	4	0	6
4	Сравнения с одним неизвестным	16	6	4	0	6
5	Сравнения второй степени	18	6	4	0	8
6	Первообразные корни и индексы	14	4	2	0	8
7	Приложение теории сравнений	10	2	0	0	8
8	Приложение теории чисел к криптографии	10	2	0	0	8
	Итого:	108	34	16	0	58

3 Образец решения нулевого варианта части А. индивидуальной домашней контрольной работы (ИДКР) по дисциплине «Алгебра и теория чисел» 2 семестр (теория чисел)

№1 *Методом разложения на простые множители найти НОД (112, 770, 1100) и НОК (112, 770, 1100).*

Решение. Разложим числа на простые множители

112	2	770	2	1100	2
56	2	385	5	550	2
28	2	77	7	275	5
14	2	11	11	55	5
7	7		1	11	11
	1				1

Таким образом, каждое из данных чисел имеет следующее разложение на простые множители:

$$112 = 2^4\times7\times1$$

$$770 = 2\times5\times7\times11\times1$$

$$1100 = 2^2\times5^2\times11\times1$$

Для отыскания НОД из множителей, входящих в разложение одного из чисел вычеркнем те, которые не входят в разложение других чисел, и найдем произведение оставшихся множителей. Получим:

$$\text{НОД }(112, 770, 1100) = 2\times 1 = 2$$

Для отыскания НОК выпишем множители, входящие в разложение одного из чисел, добавим к ним недостающие множители из разложений остальных чисел и найдем произведение получившихся множителей. Получим:

$$\text{НОК }(112, 770, 1100) = 2\times2\times2\times2\times5\times5\times7\times11\times1 = 2^4\times5^2\times7\times11\times1 = 30800$$

Ответ: НОД (112, 770, 1100) $= 2\times1 = 2$

НОК (112, 770, 1100) $= 2^4\times5^2\times7\times11\times1 = 30800$

№2 а) *Найти НОД(579, 324), используя алгоритм Евклида*

Теоретическая справка. Напомним, что алгоритм Евклида вычисления наибольшего общего делителя целых чисел a и b>0 состоит из следующих этапов. Положим $a_0 = a, a_1 = b$ и выполним последовательно деления с остатком:

$$a_0 = a_1 q_1 + a_2,\ \ 0 \le a_2 < a_1,$$

$$a_1 = a_2 q_2 + a_3,\ \ 0 \le a_3 < a_2,$$

……………………………….

$$a_{k-2} = a_{k-1} q_{k-1} + a_k,\ \ 0 \le a_k < a_{k-1},$$

$$a_{k-1} = a_k q_k.$$

Так как остатки выполняемых делений образуют строго убывающую последовательность $a_1 > a_2 > a_3 > \ldots \ge 0,$ то этот процесс обязательно остановится в результате получения нулевого остатка деления. Легко видеть, что НОД(a_0, a_1) = НОД(a_1, a_2) = … = НОД(a_{k-1}, a_k) = a_k. Значит последний ненулевой остаток a_k= НОД(a, b).

Решение. Для заданных чисел 579, 324 имеем:

Положим a_0= 579, a_1 = 324 и выполним последовательно деления с остатком a_i на a_{i+1}:

a_0= 579 = 324×1+255 = a_1q_1+a_2, a_2= 255 <a_1

a_1= 324 = 255×1+69 = a_2q_2+a_3, a_3= 69 <a_2

a_2= 255 = 69×3+48 = a_3q_3+a_4, a_4= 48 <a_3

a_3= 69 = 48×1+21 =a_4q_4+a_5, a_5= 21 <a_4

a_4= 48 = 21×2+6 = a_5q_5+a_6, a_6= 6 <a_5

a_5= 21 = 6×3+3 = a_6q_6+a_7, a_7= 3 <a_6

a_6= 6 = 3×2+0 = a_7q_7

Таким образом, НОД (579, 324) = a_7= 3

б) *Записать линейное представление НОД (579, 324)*

Решение. Для записи линейного представления НОД (579, 324) после вычисления этапов алгоритма Евклида выполним обратный проход, в каждом из которых уравнение разрешается относительно остатка a_i. В результате получаем следующую последовательность вычислений:

a_0= 579 = 324×1+255 = a_1q_1+a_2, a_2= 255 = 579 - 324×1 =$a_0 - a_1q_1$

a_1= 324 = 255×1+69 = a_2q_2+a_3, a_3= 69 = 324 - 255×1 = $a_1 - a_2q_2$

a_2= 255 = 69×3+48 = a_3q_3+a_4, a_4= 48 = 255 - 69×3 = $a_2 - a_3q_3$

a_3= 69 = 48×1+21 =a_4q_4+a_5, a_5= 21 = 69 - 48×1=$a_3 - a_4q_4$

a_4= 48 = 21×2+6 = a_5q_5+a_6, a_6= 6 = 48 - 21×2 = $a_4 - a_5q_5$

a_5= 21 = 6×3+3 = a_6q_6+a_7, a_7= 3 = 21- 6×3 = $a_5 - a_6q_6$

a_6= 6 = 3×2+0 = a_7q_7

Отсюда следует, что НОД (579, 324) = 3 и выполняются равенства:

3 = 21 - $\underline{6}$×3

3 = 21 – (48 – $\underline{21}$×2)×3

3 = 21 – (48 – (69 – $\underline{48}$×1)×2)×3

3 = 21 – (48 – (69 – (255 – $\underline{69}$×3)×1)×2)×3

3 = 21 – (48 – (69 – (255 – (324 – $\underline{255}$×1)×3)×1)×2)×3

3 = 21 – (48 – (69 – (255 – (**324** – (**579** – **324**×1)×1)×3)×1)×2)×3

Аккуратно раскрывая скобки, приводя подобные, окончательно получаем:

3= 579×(– 47) +324×84

№3 а) ***Представить данное рациональное число в виде цепной дроби***

Теоретическая справка.

С помощью алгоритма Евклида любое число можно представить в виде специальной конструкции, которая называется цепной дробью.

Рассмотрим рациональное число r, представленное в виде несократимой дроби r = $\frac{a_0}{a_1}$. Результат вычисления наибольшего общего делителя по алгоритму Евклида имеет вид:

$$a_0 = a_1 q_1 + a_2,\ \ 0 \le a_2 < a_1,$$

$$a_1 = a_2 q_2 + a_3,\ \ 0 \le a_3 < a_2,$$

……………………………….

$$a_{k-2} = a_{k-1} q_{k-1} + a_k,\ \ 0 \le a_k < a_{k-1},$$

$$a_{k-1} = a_k q_k,$$

где a_k= НОД($a_0,\ a_1$) = 1.

Эти равенства можно переписать в виде:

$$\frac{a_0}{a_1} = q_1 + \frac{a_2}{a_1},\ \frac{a_1}{a_2} = q_2 + \frac{a_3}{a_2}, \dots, \frac{a_{k-2}}{a_{k-1}} = q_{k-1} + \frac{a_k}{a_{k-1}} = \frac{a_0}{a_1} = q_{k-1} + \frac{1}{q_k}$$

Тогда рациональное число r можно представить следующим образом:

$$r = \frac{a_0}{a_1} = q_1 + \frac{a_2}{a_1} = q_1 + \frac{1}{\frac{a_1}{a_2}} = q_1 + \frac{1}{q_2 + \frac{1}{\frac{a_3}{a_2}}} = \dots = q_1 + \frac{1}{q_2 + \frac{1}{q_{k-1} + \frac{1}{q_k}}}$$

Таким образом, любая несократимая рациональная дробь $\frac{a_0}{a_1}$ может быть представлена в виде цепной дроби $\frac{a_0}{a_1} = (q_1; q_2, \dots, q_k)$ с неполными частными $q_1, q_2, \dots, q_k$, полученными в результате вычисления по алгоритму Евклида наибольшего общего делителя взаимно простых чисел $a_0,\ a_i$.

Представим рациональное число r = $\frac{18}{5}$ в виде цепной дроби.

Положим, a_0= 18, a_1= 5

$a_0 = 18 = 5 \times 3 + 3 = a_1 q_1 + a_2$, или $\frac{a_0}{a_1} = \frac{18}{5} = 3 + \frac{3}{5} = q_1 + \frac{a_2}{a_1}$,

$a_1 = 5 = 3 \times 1 + 2 = a_2 q_2 + a_3$, или $\frac{a_1}{a_2} = \frac{5}{3} = 1 + \frac{2}{3} = q_2 + \frac{a_3}{a_2}$,

$a_2 = 3 = 2 \times 1 + 1 = a_3 q_3 + a_4$, или $\frac{a_2}{a_3} = \frac{3}{2} = 1 + \frac{1}{2} = q_3 + \frac{a_4}{a_3}$,

$a_3 = 2 = 1 \times 2 + 0 = a_4 q_4$, или $\frac{a_3}{a_4} = \frac{2}{1} = 2 = q_4$

$$r = \frac{a_0}{a_1} = q_1 + \frac{a_2}{a_1} = q_1 + \frac{1}{\frac{a_1}{a_2}} = q_1 + \frac{1}{q_2 + \frac{1}{\frac{a_3}{a_2}}} = \dots = q_1 + \frac{1}{q_2 + \frac{1}{q_{k-1} + \frac{1}{q_k}}}$$

Ответ: $\frac{18}{5} = (q_1; q_2, q_3, q_4) = (3; 1,1,2) = 3 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}$

б) ***Восстановить полную последовательность подходящих дробей***

Теоретическая справка.

Для цепной дроби $\frac{a_0}{a_1} = (q_1; q_2, \dots, q_k)$ выражения

$$\delta_1 = q_1,\ \delta_2 = q_1 + \frac{1}{q_2},\ \delta_3 = q_1 + \frac{1}{q_2 + \frac{1}{q_3}},\ \delta_4 = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{q_4}}}$$

называются *подходящими дробями*.

Каждая подходящая дробь δ_i является несократимой рациональной дробью $\delta_i = \frac{P_i}{Q_i}$, числитель и знаменатель которой вычисляются по формулам:

$$P_i = q_i P_{i-1} + P_{i-2},$$

$$Q_i = q_i Q_{i-1} + Q_{i-2}$$

с начальными условиями

$$P_{-1} = 0, \quad P_0 = 1, \quad Q_{-1} = 1, \quad Q_0 = 0.$$

Вычисление числителей и знаменателей подходящих дробей оформляется в виде следующей таблицы:

I	-1	0	1	2	……	k-1	k
q_i			q_1	q_2	……	q_{k-1}	q_k
P_i	0	1	P_1	P_2	……	P_{k-1}	P_k
Q_i	1	0	Q_1	Q_2	……	Q_{k-1}	Q_k

Восстановим полную последовательность подходящих дробей числа r = $\frac{18}{5}$:

I	-1	0	1	2	3	4
q_i			3	1	1	2
P_i	0	1	3	4	7	18
Q_i	1	0	1	1	2	5

Ответ: $\delta_1 = 3, \quad \delta_2 = 3 + \frac{1}{1} = 4, \quad \delta_3 = 3 + \frac{1}{2} = \frac{7}{2}, \quad \delta_4 = \frac{18}{5}.$

№4 *Найти все решения диофантова уравнения* $23x - 15y = 13$

Теоретическая справка.

Диофантовым уравнением называются алгебраическое уравнение с целочисленными коэффициентами, решение которого отыскивается в целых числах.

Например, диофантовым уравнением является уравнение вида $ax - by = 1$ с целыми неотрицательными a, b. Если коэффициенты a, b удовлетворяют условию НОД(a, b)=1 и $\frac{P_{k-1}}{Q_{k-1}}$ - предпоследняя подходящая дробь представления числа $\frac{a}{b}$ в виде цепной дроби, то из равенств

$$P_k Q_{k-1} - P_{k-1} Q_k = (-1)^k, \qquad \frac{a}{b} = \delta_k = \frac{P_k}{Q_k}$$

следует, что

$$a(-1)^k Q_{k-1} - b(-1)^k P_{k-1} = 1,$$

т.е значения $x = (-1)^k Q_{k-1}$, $y = (-1)^k P_{k-1}$ являются целочисленными решениями уравнения $ax - by = 1$.

Таким образом, все целые решения исходного диофантова уравнения $ax - by = 1$ находится по формулам:

$$x = (-1)^k Q_{k-1} + bt,$$

$$y = (-1)^k P_{k-1} + at,$$

где t - произвольное целое число.

Все решения диофантова уравнения $ax - by = c$, имеющего взаимно простые коэффициенты a, b находятся по формулам:

$$x = (-1)^k c Q_{k-1} + bt$$

$$y = (-1)^k c P_{k-1} + at,$$

где t-произвольное целое число.

Выполним поставленную задачу: найти все решения диофантова уравнения $23x - 15y = 13$.

Решение.

Для решения диофантова уравнения $23x - 15y = 13$ вычислим числители и знаменатели подходящих дробей цепной дроби $\frac{23}{15} = (1; 1,1,7)$, применяя алгоритм Евклида:

$$a_0 = 23 = 15 \times 1 + 8 = a_1 q_1 + a_2$$

$$a_1=15 = 8\times1+7 = a_2 q_2 + a_3$$

$$a_2=8 = 7\times1+1 = a_3 q_3 + a_4$$

$$a_3=7 = 1\times7 = a_4 q_4$$

Результат вычисления числителей и знаменателей подходящих дробей цепной дроби оформим в виде следующей таблицы:

I	-1	0	1	2	3	4
q_i			1	1	1	7
P_i	0	1	1	2	3	23
Q_i	1	0	1	1	2	15

Следовательно, числитель и знаменатель предпоследней подходящей дроби есть

$$P_{k-1} = P_3 = 3$$

$$Q_{k-1} = Q_3 = 2,$$

следовательно, значения

$$x = (-1)^k Q_{k-1} = (-1)^4 \times 2 = 2,$$

$$y = (-1)^k P_{k-1} = (-1)^4 \times 3 = 3$$

являются решениями уравнения

$$23x - 15y = 13.$$

Ясно, что решением этого уравнения будут также значения

$$x = (-1)^k Q_{k-1} + bt = 2 + 15t,$$

$$y = (-1)^k P_{k-1} + at = 3 + 23t$$

для произвольного числа t.

Ответ: решение диофантова уравнения $23x - 15y = 13$ имеет вид

$$x = (-1)^k cQ_{k-1} + bt = (-1)^4 \times 13 \times 2 + 15t = 26 + 15t$$

$$y = (-1)^k cP_{k-1} + at = (-1)^4 \times 13 \times 3 + 23t = 39 + 23t,$$

где t - произвольное число.

№5 *Найти мультипликативно обратный элемент для вычета a по модулю m*

а) используя алгоритма Евклида;

б) используя теорему Ферма-Эйлера.

***а)** Теоретическая справка.*

Мультипликативно обратным элементом по модулю m для элемента a называется число, удовлетворяющее равенству $ax \equiv xa \equiv 1(mod\, m)$, такое число обозначается a^{-1}.

Способ вычисления мультипликативно обратного элемента по модулю m, основанный на алгоритме Евклида, следует из свойства числителей и знаменателей двух последних подходящих дробей цепной дроби $\frac{a}{m} = (q_1; q_2, \ldots, q_k)$. В самом деле, из равенств

$$P_k Q_{k-1} - P_{k-1} Q_k = (-1)^k, \qquad \frac{a}{b} = \delta_k = \frac{P_k}{Q_k}$$

в силу НОД(a, m) = 1 следует, что

$$a(-1)^k Q_{k-1} - m(-1)^k P_{k-1} = 1, \text{ т.е значения}$$

$$x = (-1)^k Q_{k-1}\,, \; y = (-1)^{k+1} P_{k-1}$$

являются целочисленными решениями уравнения $ax - my = 1$ и, значит, $a^{-1} = (-1)^k Q_{k-1}$ для знаменателя Q_{k-1} предпоследней подходящей дроби представления числа $\frac{a}{m}$ в виде цепной дроби.

Используя алгоритма Евклида, найдем мультипликативно обратный элемент для вычета a=25 по модулю m=42.

Решение. Представим рациональное число r = $\frac{25}{42}$ в виде цепной дроби (0; 1, 1, 2, 8), так как по алгоритму Евклида получаем:

$a_0 = 25, \qquad a_1 = 42$

$a_0 = 25 = 42 \times 0 + 25 = a_1 q_1 + a_2,$ или $\frac{a_0}{a_1} = \frac{25}{42} = 0 + \frac{25}{42} = q_1 + \frac{a_2}{a_1},$

$a_1 = 42 = 25 \times 1 + 17 = a_2 q_2 + a_3$, или $\frac{a_1}{a_2} = \frac{42}{25} = 1 + \frac{17}{25} = q_2 + \frac{a_3}{a_2}$,

$a_2 = 25 = 17 \times 1 + 8 = a_3 q_3 + a_4$, или $\frac{a_2}{a_3} = \frac{25}{17} = 1 + \frac{8}{17} = q_3 + \frac{a_4}{a_3}$,

$a_3 = 17 = 8 \times 2 + 1 = a_4 q_4 + a_5$, или $\frac{a_3}{a_4} = \frac{17}{8} = 2 + \frac{1}{8} = q_4 + \frac{a_5}{a_4}$,

$a_3 = 8 = 1 \times 8 + 0 = a_5 q_5$, или $\frac{a_4}{a_5} = \frac{8}{1} = 8 = q_5$.

Результат вычисления числителей и знаменателей подходящих дробей цепной дроби $\frac{25}{42} = (0; 1, 1, 2, 8)$ оформим в виде следующей таблицы:

I	-1	0	1	2	3	4	5
q_i			0	1	1	2	8
P_i	0	1	0	1	1	3	25
Q_i	1	0	1	1	2	5	42

Вычислим элементы таблицы по формулам:

$$P_i = P_i - 1 \times q_i + P_i - 2$$

$$Q_i = Q_i - 1 \times q_i + Q_i - 2$$

$$Q_{k-1} = 5$$

Для вычета $a = 25$ мультипликативно обратный элемент 25^{-1} по модулю $m = 42$ вычисляется по формуле

$$a^{-1} = (-1)^k Q_{k-1} = (-1)^5 \times 5 = -5$$

Так как необходимо наименьшее положительное число, то $-5 + 42 = 37$

Проверка:

$$25 \times 37 = 925$$

$$925/42 = 22 \text{ (ост. 1)}$$

$$925 = 42 \times 22 + 1$$

$$25 \times 37 \equiv 1 (mod\, 42)$$

Ответ: для вычета a = 25 мультипликативно обратный элемент 25^{-1} по модулю m= 42 равен 37.

б) Используя теорему Ферма-Эйлера, найдем мультипликативно обратный элемент для вычета а=25 по модулю m=42.

Теоретическая справка. Теорема Ферма-Эйлера утверждает, что для взаимно простых чисел a и m выполняется свойство $a^{\varphi(m)} \equiv 1 (mod\, m)$, где $\varphi(m)$ - значение функции Эйлера, равное по определению количеству натуральных чисел $n \leq m$, которые взаимно простые с числом m.

Так как формулу Ферма-Эйлера можно представить в виде $aa^{\varphi(m)-1} \equiv 1 (mod\, m)$, то по определению $a^{-1} = a^{\varphi(m)-1}$.

Решение. Найдем значение функции Эйлера от $m = 42$, для этого разложим число m на простые множители

$$\begin{array}{r|l} 42 & 2 \\ 21 & 3 \\ 7 & 7 \\ 1 & \end{array}$$

$$\varphi(42) = (2-1) \times (3-1) \times (7-1) = 1 \times 2 \times 6 = 12$$

$$a^{-1} = a^{\varphi(42)-1} = a^{11}$$

$$a^{-1} = 25^{11} (mod\, 42)$$

Разложив 25^{11} как $25^2 \times 25^{10}$, имеем

$$a^{-1} = 37^5 \times 25 \text{ (mod 42)}$$

Разложив 37^5 как $(37^2)^2 \times 37$, получим

$$a^{-1} = 25^2 \times 37 \times 25 \text{ (mod 42)}$$

$$a^{-1} = 37 \times 37 \times 25 \text{(mod 42)}$$

$$a^{-1} = 25 \times 25 \text{(mod 42)}$$

$$a^{-1} = 37 \text{(mod 42)}$$

Ответ: для вычета a= 25 мультипликативно обратный элемент 25^{-1} по модулю $m = 42$ равен 37.

№6 ***Решить систему линейных сравнений***

$$\begin{cases} x \equiv 3 \pmod 7 \\ x \equiv 1 \pmod 3 \\ x \equiv 3 \pmod 2 \\ x \equiv 8 \pmod{13} \end{cases}$$

Решение. Так как числа 7, 3, 2, 13 попарно взаимно простые, то данная система линейных сравнений имеет единственное неотрицательное решение по модулю M

$$M = 7\times3\times2\times13 = 546$$

$$M_i = M/m_i$$

$$M_1 = M/m_1 = 546/7 = 78$$

$$M_2 = M/m_2 = 546/3 = 182$$

$$M_3 = M/m_3 = 546/2 = 273$$

$$M_4 = M/m_4 = 546/13 = 42$$

Поскольку числа 78 и 7 взаимно простые, сравнение $78x \equiv 3 \pmod 7$ равносильно сравнению

$$x \equiv 3 \pmod 7$$

и имеет решение $z_1 = 3$

Проверка:

$$\left.\begin{matrix} 3 - 3 = 0 \\ 0 \vdots 7 \end{matrix}\right\} \Rightarrow z_1 = 3 \text{ - корень}$$

Поскольку числа 182 и 3 взаимно простые, сравнение $128x \equiv 1 \pmod 3$ равносильно сравнению

$$2x \equiv 1 \pmod 3$$

и имеет решение $z_2 = 2$

Проверка:

$$\left.\begin{matrix} 1-4=-3 \\ -3 \vdots 3 \end{matrix}\right\} \Rightarrow z_2 = 2 \text{ - корень}$$

Поскольку числа 273 и 2 взаимно простые, сравнение $273x \equiv 3 (\mathrm{mod}\ 2)$равносильно сравнению

$$x \equiv 3 (\mathrm{mod}\ 2)$$

и имеет решение $z_3 = 1$

Проверка:

$$\left.\begin{matrix} 3-1=2 \\ 2 \vdots 2 \end{matrix}\right\} \Rightarrow z_3 = 1 \text{ - корень}$$

Поскольку числа 42 и 13 взаимно простые, сравнение $42x \equiv 8 (\mathrm{mod}\ 13)$равносильно сравнению

$$3x \equiv 8 (\mathrm{mod}\ 13)$$

и имеет решение $z_4 = 7$

Проверка:

$$\left.\begin{matrix} 8-21=-13 \\ -13 \vdots 13 \end{matrix}\right\} \Rightarrow z_4 = 7 \text{ - корень}$$

Значит, решением данной системы линейных сравнений является остаток по модулю 546 числа x.

Найдем x: $x = M_1z_1+M_2z_2+ M_3z_3+M_4z_4$

$$x = 78\times3+182\times2+273\times1+42\times7 = 234+364+273+294 = 1165.$$

Решением данной системы линейных сравнений является остаток по модулю 546 числа x = 1165, т.е $x\equiv73(\mathrm{mod}\ 546)$

$$1165 = 546\times2+73$$

$$1165(\mathrm{mod}\ 546) \equiv 73(\mathrm{mod}\ 546)$$

$$\begin{cases} 73 \equiv 3 (\mathrm{mod}\ 7) \\ 73 \equiv 1 (\mathrm{mod}\ 3) \\ 73 \equiv 3 (\mathrm{mod}\ 2) \\ 73 \equiv 8 (\mathrm{mod}\ 13) \end{cases}$$

Проверка:

1) $73 \equiv 3 \pmod 7$; 3 - 73= - 70; -70⋮7.
2) $73 \equiv 1 \pmod 3$; 1 - 73= - 72; -72⋮3.
3) $73 \equiv 3 \pmod 2$; 3 - 73= - 70; -70⋮2.
4) $73 \equiv 8 \pmod{13}$; 8 - 73= - 65; -65⋮13.

Ответ: x = 73 - наименьшее положительное целочисленное решение.

4 Задания индивидуальной домашней контрольной работы (ИДКР №2)

4.1 ИДКР №2, *часть А*

№1 ***Методом разложения на простые множители найти НОД (a, b, c) и НОК (a, b, c)***

№	*a*	*b*	*c*	*№*	*a*	*b*	*c*
1.	150	8085	870	**11.**	870	570	4389
2.	1155	1610	798	**12.**	570	2145	4389
3.	4389	308	870	**13.**	1078	870	798
4.	4389	798	1197	**14.**	1610	150	798
5.	1197	870	2145	**15.**	798	8085	1155
6.	308	8085	870	**16.**	870	1155	1197
7.	2145	4389	570	**17.**	308	870	1197
8.	1197	570	798	**18.**	798	8085	570
9.	1155	870	150	**19.**	4389	570	798
10.	570	1610	1078	**20.**	1197	1610	870

№2 а) ***Найти НОД (a, b), используя алгоритма Евклида;***
б) ***Записать линейное представление НОД (a, b).***

№	***A***	***b***	**№**	***a***	***b***	**№**	***a***	***B***
1.	308	870	**8.**	870	570	**15.**	150	8085
2.	798	8085	**9.**	570	2145	**16.**	1155	1610
3.	4389	570	**10.**	1078	870	**17.**	4389	308
4.	1197	1610	**11.**	1610	150	**18.**	4389	798
5.	1197	570	**12.**	798	8085	**19.**	1197	870
6.	1155	870	**13.**	870	1155	**20.**	308	8085
7.	2145	4389	**14.**	570	1610			

№3 а) ***Представить данное рациональное число r в виде цепной дроби;***

б) ***Восстановить полную последовательность подходящих дробей числа r.***

№	***r***	**№**	***r***
1.	35/6	**11.**	14/9
2.	16/5	**12.**	28/9
3.	14/9	**13.**	32/7
4.	24/7	**14.**	21/8
5.	16/3	**15.**	16/5
6.	24/5	**16.**	34/5
7.	28/7	**17.**	24/9
8.	22/7	**18.**	14/3
9.	13/4	**19.**	32/5
10.	25/6	**20.**	16/9

№4 ***Найти все решения диофантова уравнения*** $a\,x - by = c$

№	a	b	c	№	a	b	c
1.	21	13	7	**11.**	27	14	13
2.	25	7	8	**12.**	23	16	8
3.	27	8	9	**13.**	27	15	11
4.	23	14	7	**14.**	29	13	8
5.	31	15	13	**15.**	28	15	12
6.	29	16	9	**16.**	29	15	7
7.	21	15	11	**17.**	27	13	9
8.	27	15	11	**18.**	21	13	7
9.	29	13	8	**19.**	25	7	8
10.	28	15	12	**20.**	27	8	9

№5 ***Найти мультипликативно обратный элемент для вычета*** a ***по модулю*** m

а) используя алгоритма Евклида;

б) используя теорему Ферма-Эйлера.

№	a	m	№	a	m	№	a	m
1.	25	40	**8.**	25	44	**15.**	28	40
2.	26	42	**9.**	26	38	**16.**	29	42
3.	28	38	**10.**	28	35	**17.**	30	38
4.	29	35	**11.**	29	42	**18.**	31	35
5.	30	42	**12.**	30	44	**19.**	25	40
6.	31	44	**13.**	31	40	**20.**	26	44
7.	30	19	**14.**	30	44			

№6 ***Решить систему линейных сравнений:***

$$\begin{cases} x \equiv b_1 (\mathrm{mod}\, m_1) \\ x \equiv b_2 (\mathrm{mod}\, m_2) \\ x \equiv b_3 (\mathrm{mod}\, m_3) \end{cases}$$

№	b_1	b_2	b_3	m_1	m_2	m_3
1.	3	4	5	15	5	13
2.	4	5	4	9	15	12
3.	5	6	3	2	9	3
4.	6	7	4	4	2	15
5.	7	6	7	3	4	9
6.	6	5	6	2	3	2
7.	5	4	5	6	2	4
8.	4	3	4	11	6	3
9.	3	4	6	12	11	2
10.	4	7	7	4	12	6
11.	7	6	6	2	4	11
12.	6	5	5	4	2	12
13.	5	4	4	6	4	4
14.	4	6	3	2	6	2
15.	6	4	4	5	2	4
16.	4	3	7	6	5	6
17.	3	2	6	11	6	2
18.	2	9	7	13	11	5
19.	9	8	6	12	13	6
20.	8	3	5	3	12	11

4.2 ИДКР №2,часть В

№7 *Решить сравнение:*

7.1 $888x^{963} - 101x^{404} + 52x^{211} + 88x^{323} + 119 \equiv 0 \pmod 7$;
7.2 $883x^{963} - 106x^{484} + 59x^{241} + 87x^{233} + 84 \equiv 0 \pmod 5$;
7.3 $445x^{526} + 43x^{264} - 89x^{263} + 226x^{262} + 102 \equiv 0 \pmod 7$;
7.4 $803x^{396} - 601x^{484} + 55x^{221} - 83x^{105} + 34 \equiv 0 \pmod 7$;
7.5 $283x^{283} - 601x^{601} + 55x^{55} - 33x^{33} + 28 \equiv 0 \pmod 5$;
7.6 $340x^{412} + 120x^{210} - 152x^{149} + 296x^{142} + 32 \equiv 0 \pmod 7$;
7.7 $288x^{279} + 604x^{605} + 550x^{55} - 33x^{33} + 28 \equiv 0 \pmod 5$;
7.8 $999x^{577} - 171x^{349} - 256x^{286} - 102x^{103} - 92 \equiv 0 \pmod 5$;
7.9 $483x^{532} + 50x^{270} - 82x^{269} + 226x^{262} + 102 \equiv 0 \pmod 7$;
7.10 $881x^{969} - 108x^{410} + 59x^{211} + 88x^{323} + 119 \equiv 0 \pmod 7$;
7.11 $152x^{343} - 704x^{201} + 105x^{75} - 102x^{29} + 2317 \equiv 0 \pmod 5$;
7.12 $883x^{963} - 106x^{484} + 59x^{241} + 87x^{233} + 84 \equiv 0 \pmod 5$;
7.13 $377x^{545} - 102x^{293} - 37x^{243} + 63x^{65} + 129 \equiv 0 \pmod 5$;
7.14 $338x^{329} + 284x^{285} - 131x^{130} + 103x^{103} - 84x^{84} + 53 \equiv 0 \pmod 5$;
7.15 $741x^{909} - 311x^{530} + 122x^{331} + 81x^{203} + 84 \equiv 0 \pmod 7$;
7.16 $999x^{577} - 171x^{349} - 256x^{286} - 102x^{103} - 92 \equiv 0 \pmod 5$;
7.17 $283x^{283} - 601x^{601} + 55x^{55} - 33x^{33} + 28 \equiv 0 \pmod 5$;
7.18 $333x^{333} - 281x^{281} + 134x^{134} + 103x^{103} - 84x^{84} + 53 \equiv 0 \pmod 5$;
7.19 $1003x^{573} + 174x^{345} - 251x^{282} - 102x^{103} + 101x^{48} - 2 \equiv 0 \pmod 5$;
7.20 $305x^{406} + 113x^{204} - 159x^{143} + 296x^{42} + 32 \equiv 0 \pmod 7$.

№8 *Решить сравнение:*

8.1 $19x^{25} \equiv 39 \pmod{61}$;
8.2 $44x^{49} \equiv 48 \pmod{71}$;
8.3 $42x^{25} \equiv 22 \pmod{61}$;
8.4 $27x^{49} \equiv 23 \pmod{71}$;
8.5 $16x^{18} \equiv 24 \pmod{97}$;
8.6 $29x^{42} \equiv 10 \pmod{61}$;
8.7 $112x^{40} \equiv 56 \pmod{89}$;
8.8 $178x^{18} \equiv 73 \pmod{97}$;
8.9 $77x^{18} \equiv 84 \pmod{67}$;
8.10 $155x^{40} \equiv 33 \pmod{89}$;

8.11 $90x^{42} \equiv 10 \pmod{61}$;
8.12 $133x^{18} \equiv 24 \pmod{97}$;
8.13 $77x^{18} \equiv 84 \pmod{67}$;
8.14 $155x^{40} \equiv 33 \pmod{89}$;
8.15 $23x^{40} \equiv 56 \pmod{89}$;
8.16 $29x^{42} \equiv 10 \pmod{61}$;
8.17 $81x^{18} \equiv 73 \pmod{97}$;
8.18 $66x^{40} \equiv 33 \pmod{89}$;
8.19 $10x^{18} \equiv 17 \pmod{67}$;
8.20 $19x^{25} \equiv 39 \pmod{61}$.

№9 Решить сравнение по составному модулю.

9.1 $x^3 - 17x^2 + 66x + 178 \equiv 0 \pmod{250}$;
9.2 $x^3 + 2x^2 + 3x + 2 \equiv 0 \pmod{440}$;
9.3 $x^4 + 4x^3 + 5x - 58 \equiv 0 \pmod{375}$;
9.4 $5x^2 + 7x + 2 \equiv 0 \pmod{36}$;
9.5 $18x^4 + 3x + 6 \equiv 0 \pmod{144}$;
9.6 $x^3 - 12x^2 + 12x - 55 \equiv 0 \pmod{135}$;
9.7 $x^3 - 20x^2 - 26x + 45 \equiv 0 \pmod{135}$;
9.8 $x^3 - 16x^2 - 5x + 20 \equiv 0 \pmod{56}$;
9.9 $x^5 - 6x^4 + 2x^3 - 7x^2 + 21x + 392 \equiv 0 \pmod{1372}$;
9.10 $x^4 + x^3 - 6x^2 + 15x + 45 \equiv 0 \pmod{1323}$;
9.11 $x^3 + x^2 + 27x - 42 \equiv 0 \pmod{2025}$;
9.12 $x^4 - 2x^2 - 2x + 16 \equiv 0 \pmod{1120}$;
9.13 $x^3 + 6x + 20 \equiv 0 \pmod{1000}$;
9.14 $x^3 + x^2 + 4x + 4 \equiv 0 \pmod{800}$;
9.15 $18x^3 + 3x + 18 \equiv 0 \pmod{288}$;
9.16 $x^3 + 5x \equiv 0 \pmod{400}$;
9.17 $18x^3 + 3x + 18 \equiv 0 \pmod{288}$;
9.18 $4x^5 + 3x + 9 \equiv 0 \pmod{288}$;
9.19 $5x^4 + 2x + 12 \equiv 0 \pmod{216}$;
9.20 $31x^4 + 57x^3 + 96x + 191 \equiv 0 \pmod{225}$;

№ 10 Найти все целые решения (x, y) заданного уравнения, удовлетворяющего заданному условию.

10.1 Найдите все целые решения (*x*, *y*) уравнения $x^2 - 3y^2 = \pm 1$, удовлетворяющие условию $|x| \leq 220$.

10.2 Найдите все целые решения (*x*, *y*) уравнения $x^2 - Dy^2 = \pm 1$, удовлетворяющие условию *x*, *y* ϵ $[-200, 200]$, если $\sqrt{D}$ = $[3, (1, 6)]$.

10.3 Найдите все целые решения (*x*, *y*) уравнений $x^2 - 8y^2 = \pm 1$, удовлетворяющие условию $|x| \leq 95$.

10.4 Найдите все целые решения (*x*, *y*) уравнения $x^2 - Dy^2 = \pm 1$, удовлетворяющие условию $|y| \leq 300$, если $\sqrt{D}$ = $[5, (5, 10)]$.

10.5 Найдите все целые решения (*x*, *y*) уравнения $x^2 - 32y^2 = \pm 1$, удовлетворяющие условию $|x| \leq 350$.

10.6 Найдите все целые решения (*x*, *y*) уравнения $x^2 - Dy^2 = \pm 1$, удовлетворяющие условию $|x| \leq 350$, если $\sqrt{D}$ = $[8, (2, 16)]$.

10.7 Найдите все целые решения (*x*, *y*) уравнений $x^2 - 27y^2 = \pm 1$, удовлетворяющие условию *x*,*y* ϵ $[-250, 100]$.

10.8 Найдите все целые решения (*x*, *y*) уравнения $x^2 - 11y^2 = \pm 1$, удовлетворяющие условию $|y| \leq 100$, если $\sqrt{D}$ = $[2, (2, 4)]$.

10.9 Найдите все целые решения (*x*, *y*) уравнения $x^2 - 99y^2 = \pm 1$, удовлетворяющие условию *x*,*y* ϵ $[-90, 90]$.

10.10 Найдите все целые решения (*x*, *y*) уравнения
$x^2 - 24y^2 = \pm 1$, удовлетворяющие условию *x*,*y* ϵ $[-100, 100]$.

10.11 Найдите все целые решения (*x*, *y*) уравнения $x^2 - Dy^2 = \pm 1$, удовлетворяющие условию $|y| \leq 200$, если $\sqrt{D}$ = $[6, (4, 12)]$.

10.12 Найдите все целые решения (*x*, *y*) уравнения $x^2 - 6y^2 = \pm 1$, удовлетворяющие условию *x*,*y* ϵ $[-150, 100]$.

10.13 Найдите все целые решения (*x*, *y*) уравнения $x^2 - Dy^2 = \pm 1$, удовлетворяющие условию $|x| \leq 100$, если $\sqrt{D}$ = $[2, (2, 4)]$.

10.14 Найдите все целые решения (*x*, *y*) уравнения $x^2 - 44y^2 = \pm 1$, удовлетворяющие условию *x*,*y* ϵ $[-200, 200]$.

10.15 Найдите все целые решения (*x*, *y*) уравнения $x^2 - 60y^2 = \pm 1$, удовлетворяющие условию *x*,*y* ϵ $[-220, 220]$.

10.16 Найдите все целые решения (*x*, *y*) уравнения $x^2 - Dy^2 = \pm 1$, удовлетворяющие условию *x*, *y* ϵ $[-200, 200]$, если $\sqrt{D}$ = $[3, (3, 6)]$.

10.17 Найдите все целые решения (*x*, *y*) уравнения $x^2 - 15y^2 = \pm 1$, удовлетворяющие условию *x*,*y* ϵ $[-220, 1200]$.

10.18 Найдите все целые решения (*x, y)* уравнений $x^2 - 108y^2 = \pm 1$, удовлетворяющие условию *x,y* ϵ $[-100, 210]$.

10.19 Найдите все целые решения (*x, y)* уравнения $x^2 - 96y^2 = \pm 1$, удовлетворяющие условию $|x| \leq 100$.

10.20 Найдите все целые решения (*x, y)* уравнения $x^2 - Dy^2 = \pm 1$, удовлетворяющие условию *x,y* ϵ $[-11, 100]$, если $\sqrt{D}$ = $[4, (1, 8)]$.

5 Дополнительные задачи

Делимость целых чисел

1 Показать, что *n (n* + 1)(2*n* + 1), где *n* - натуральное число, делится на b.

2 Показать, что *n* (n^2 + 5), где *n* - натуральное число, делится на 6.

3 Показать, что если числитель дроби есть разность квадратов двух нечетных чисел, а знаменатель - сумма квадратов тех же чисел, то такая дробь всегда сократима на 2, но несократима на 4.

4 Найти четырехзначное число, являющееся точным квадратом, у которого цифра тысяч одинакова с цифрой десятков, а цифра сотен на 1 больше цифры единиц.

5 Если остаток от деления некоторого числа на 9 есть одно из чисел 2, 3, 5, 6, 8, то это число не может быть точным квадратом.

Наибольший общий делитель и наименьшее общее кратное

6 Сумма двух чисел 667, а отношение НОК к их НОД равно 120. Найти эти числа.

7 Показать, что для любых натуральных a и b имеет место равенство:

(a, b) = (5a + 3b, 13a + 8b)

8 Показать, что при любых натуральных *m* и *n* (m^4 - n^4) делится на 30.

9 Сумма двух чисел 667, а отношение НОК к их НОД равно 120. Найти эти числа.

10 Показать, что при любом натуральном *n* произведение *(n + 1) (n + 2) ... (n + n)* делится на 2^n.

Вычеты. Системы вычетов

11 Показать, что числа 19, 23, 25, -19 составляют приведенную систему вычетов по модулю m = 12.

12 Показать, что числа 11, -1, 17,-19 составляют приведенную систему вычетов по модулю *m = 8*.

13 Показать, что числа 13, -13, 29, -9 составляют приведенную систему вычетов по модулю $m = 10$.

14 Найти наименьшие неотрицательные, наименьшие по абсолютной величине неположительные и абсолютно наименьшие вычеты чисел 24, 14 , 25, 37, -8, -19,-40 по модулю m = 6. Ко скольким различным классам принадлежат данные числа по данному модулю? Какие числа из данных принадлежат к одному и тому же классу по данному модулю?

15.Найти наименьшие неотрицательные, наименьшие по абсолютной величине неположительные и абсолютно наименьшие вычеты числа 100 по модулям: 5, 7, 11, 25, 120, 200.

Теоремы Эйлера и Ферма

16 Доказать, что если $a^p \equiv \pm 1 (\text{mod } p)$, то тогда и $a^p = \pm 1 (\text{mod } p^2)$ (p - число простое).

17 Если p и q - неравные между собой простые числа, то
$p^{q-1} + q^{p-1} \equiv 1 \ (\text{mod } pq)$.

18 Доказать, что при любом целом $xx^7 = x$ (mod 42).

19 Показать, что если $m > 1$ - нечетное число, то $2^{\varphi(m)-1}$ дает при делении на m остаток, равный $m - \left[\frac{m}{2}\right]$.

20 Найти остаток от деления $4^{\varphi(m)-1}$ на нечетное число $m > 1$.

Сравнения

21 Показать, что $2^{11\cdot 31} \equiv 2 \ (\text{mod } 11\cdot 31)$.

22 Найти остаток от деления $1532^6 - 1$ на 9.

23 Доказать, что если p - простое число, то $C_{p-1}^{k} \equiv (-1)^k (\text{mod } p)$.

24 Доказать, что если $a \equiv b (\text{mod } p^n)$, то $a^p \equiv b^p (\text{mod } p^{n+1})$, p - число простое.

25 Показать, что если n - нечетное число, то $n^2 - 1 = 0 (\text{mod } 8)$.

6 Рекомендуемая литература

1 Балюкевич, Э. Л. Алгебра и теория чисел. Учебно-методический комплекс [Электронный ресурс] / Балюкевич Э. Л., Романников А. Н., Алферова З. В. - Евразийский открытый институт, 2011.

2 Банникова, Т.М., Баранова, Н.А. «Основы теории чисел»(учебно - методическое пособие). – Ижевск, 2009.

3 Башмакова, И.Г. Диофант и диофантовы уравнения [Текст]. – М.: «Наука», 1972 г. - 68 с.

4 Веселова, Л.В. Теория чисел / Л.В. Веселова. – Казань.: КНИТУ, 2012.

5 Виноградов, И.М. Основы теории чисел / И.М. Виноградов. – М.: Наука, 1981.

6 Деза, Е.И., Котова, Л.В. Сборник задач по теории чисел (112 задач с подробными решениями): Учебное пособие. – М.: Книжный дом "ЛИБРОКОМ", 2012. – 224 с.

7 Куликов, Л.Я. «Алгебра и теория чисел». – М.: Высшая школа, 1979.

8 Молчанов, В. А. Алгебра и теория чисел [Текст] : учеб. пособие для вузов / В.А. Молчанов; М-во образования и науки Рос. Федерации, Гос. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т". - Оренбург : ГОУ ОГУ, 2009. - 194 с.

9 Нечаев, В.И. Элементы криптографии. Основы защиты информации / В.И. Нечаев. – М.: Высшая школа, 1999.

10 Сизый, С.В. Лекции по теории чисел / С.В. Сизый. – М.: ФИЗМАТЛИТ, 2007.

Периодические издания

1Алгебра и анализ: журнал.-М.:Агенство"Роспечать".

2 Дискретная математика: журнал. - М.: Агенство "Роспечать".

3 Алгебра и логика: журнал. - М.: Агенство "Роспечать".

4 Математика: реферативный журнал. - М.: Агенство "Роспечать".

Интернет-ресурсы

1 http://www.mathelp.spb.ru - Лекции по высшей математике, учебники on-line, математические web-сервисы.

2 http://www.pm298.ru/mfizika.php математические формулы по высшей математике, примеры решения математических задач.

3 http://www.matburo.ru/st_subject.php?p=vm - Учебники, лекции, методические пособия по высшей математике.

7 Использованная литература

1 Виноградов, И.М. Основы теории чисел / И.М. Виноградов. – М.: Наука, 1981.

2 Деза, Е.И., Котова, Л.В. Сборник задач по теории чисел (112 задач с подробными решениями): Учебное пособие. – М.: Книжный дом "ЛИБРОКОМ", 2012. – 224 с.

3 Молчанов, В. А. Алгебра и теория чисел [Текст] : учеб. пособие для вузов / В. А. Молчанов; М-во образования и науки Рос. Федерации, Гос. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т". - Оренбург : ГОУ ОГУ, 2009. - 194 с. - Библиогр.: с. 189.