Министерство образования Республики Беларусь
БЕЛОРУССКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Кафедра «Инженерная математика»

Т.Г. Крупенкова

КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Учебно-методическое пособие
для студентов специальности 1-38 02 03
«Техническое обеспечение безопасности»
специализации 1-38 02 03 02 «Аппаратно-программные средства
защиты компьютерной информации»

В 2 частях

Часть 1

Учебное электронное пособие

Минск
БНТУ
2012

УДК 512.624.95:378.147.091.3

Рецензенты:

И.Е. Зуйков, заведующий кафедрой «Информационно-измерительная техника и технология» БНТУ, доктор физико-математических наук, профессор;

В.А. Липницкий, заведующий кафедрой «Высшая математика и физика» Военной академии Республики Беларусь, доктор технических наук, профессор

Учебно-методическое пособие служит для практического освоения студентами материала специального курса «Криптографические средства защиты информации». В нем изложены математические основы криптографии. Приведен материал для практических, лабораторных и самостоятельных занятий по теории чисел, теории групп, кольцам классов вычетов. Пособие практически знакомит с основными ассиметричными криптографическими системами.

Белорусский национальный технический университет
Пр-т Независимости, 65, г. Минск, Республика Беларусь
Тел (017) 292-77-52 факс (017) 292-91-37
Регистрационный № ЭИ БНТУ/ПСФ85-55.2012

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Курс «Криптографические средства защиты информации» является относительно новым, находится в динамике становления и развития в соответствии с технологической революцией и потребностями времени, требует изучения новых разделов математики, не вошедших в классический курс «Высшая математика» – необходимую базу высшего технического образования. Поэтому на кафедре инженерной математики разработан курс «Криптографические средства защиты информации» отнесен к разделу «Специальные главы высшей математики». На протяжении ряда лет этот курс успешно читается студентам БНТУ специальности «Техническое обеспечение безопасности».

В данном учебно-методическом пособии изложен необходимый теоретический материал, но опыт показывает, что глубокое и надежное усвоение нового материала невозможно без его основательной проработки на практических и лабораторных занятиях, поэтому данное издание предназначено для их проведения. Предлагается рабочая модель семи практических и лабораторных занятий по основным темам курса. При этом, в зависимости от сложившейся традиции, лабораторные задания можно рассматривать как домашние – для самостоятельного индивидуального изучения.

Данное издание будет полезно не только студентам названной специальности, но и всем, кто изучает проблематику современной криптографии.

Лабораторная работа № 1
ИСТОРИЧЕСКИЕ ШИФРЫ

Цель работы: изучение некоторых исторических шифров.

Необходимые теоретические сведения

Рассмотрим основные исторические криптосистемы защиты информации от несанкционированного доступа.

Шифр Цезаря

В I веке н. э. Юлий Цезарь во время войны с галлами, переписываясь со своими друзьями в Риме, заменял в сообщении первую букву латинского алфавита (A) на четвертую (D), вторую (B) – на пятую (E), наконец, последнюю – на третью в соответствии со следующей таблицей:

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
D	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*

В русском варианте эта таблица выглядит так:

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ

Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Ы	Ь	Э	Ю	Я	А	Б	В

Шифр Цезаря входит в класс шифров, называемых «подстановка» или «простая замена». Это такой шифр, в котором каждой букве алфавита соответствует буква, цифра, символ или какая-нибудь их комбинация.

Сообщение об одержанной победе выглядело так:

Пример 1.1.

YHQL	*YLGL*	*YLFL*	(ЛАТ.)
ТУЛЫИО	ЦЕЛЖЗО	ТСДЗЖЛО	(РУС.)
Пришёл,	увидел,	победил.	

(Ю. Цезарь. Донесение Сенату о победе над понтийским царем).

Тарабарская грамота

Первое известное применение тайнописи в России относится к XIII в. Эту систему называли «тарабарской грамотой». В этой системе согласные буквы заменяются по схеме:

Б	В	Г	Д	Ж	З	К	Л	М	Н
Щ	Ш	Ч	Ц	Х	Ф	Т	С	Р	П

При шифровании буквы, расположенные на одной вертикали, переходят одна в другую. Остальные буквы остаются без изменения.

Пример 1.2. Так выглядит известная пословица, записанная «тарабарской грамотой»:

М Ы Щ А Л Ч О С О Ш Ы Ч П И Ё К

Рыба с головы гниёт.

Таблица Виженера (1576 г.)

а	**б**	**в**	**г**	**д**	**е**	**ё**	**ж**	**з**	**и**	**й**	**к**	**л**	**м**	**н**	**о**	**п**	**р**	**с**	**т**	**у**	**ф**	**х**	**ц**	**ч**	**ш**	**щ**	**ъ**	**ы**	**ь**	**э**	**ю**	**я**
б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а
в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б
г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в
д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г
е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д

ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е
ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё
з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж
и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з
й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и
к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й
л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к
м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л
н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м
о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н
п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о
р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п
с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р
т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с
у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т
ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у
х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф
ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х
ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц
ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч
щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш
ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ
ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы
э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь
ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э
я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю

В процессе шифрования (и дешифрования) часто используется так называемая «таблица Виженера», которая устроена следующим образом: в первой строке выписывается весь алфавит, в каждой следующей осуществляется циклический сдвиг на одну букву. Так получается квадратная таблица, число строк которой равно числу столбцов и равно числу букв в алфавите.

Чтобы зашифровать какое-нибудь сообщение, поступают следующим образом. Выбирается слово-лозунг и подписывается с повторением над буквами сообщения.

Чтобы получить шифрованный текст, находят очередной знак лозунга, начиная с первого, в вертикальном алфавите, а соответствующий ему знак сообщения в горизонтальном.

На пересечении выделенных столбца и строки находим зашифрованную букву.

Пример 1.3. Зашифруем фразу «торопись медленно» с помощью слова-лозунга «море»:

м	о	р	е	м	о	р	е	м	о	р	е	м	о	р	е
т	о	р	о	п	и	с	ь	м	е	д	л	е	н	н	о
я	э	б	у	ь	ч	в	б	щ	у	ф	р	с	ь	ю	у

Постолбцовая транспозиция (XIX век)

К классу «перестановка» относится шифр «маршрутная транспозиция» и его вариант «постолбцовая транспозиция». В данный прямоугольник $[n \times m]$ вписывается сообщение по строкам. Шифрованный текст найдем, если будем выписывать буквы в порядке следования столбцов.

Пример 1.4. Зашифруем фразу «Каждая собака – хозяин у своей двери».

Решение. Фраза содержит 30 символов с учетом тире. Ее можно записать в прямоугольники размером 2×15; 3×10; 5×6 и т. д. Выберем прямоугольник размером 5×6.

1	2	3	4	5	6
к	а	ж	д	а	я
с	о	б	а	к	а
–	х	о	з	я	и
н	у	с	в	о	е
й	д	в	е	р	и

Выписываем шифрованное сообщение по столбцам:

кс–ний аохуд жбосв дазве акяор яаиеи.

Задания для аудиторной работы

Задание 1. Прочитать текст, записанный с помощью шифра Цезаря:

а) еогфхя – ахс ефзёжг пгёлв олщзжзмфхег;

б) тусхлерцб фхсусрц ргжс еюфоцылегхя, нгн дю срг рз дюог тусхлерг.

Задание 2. Расшифровать «тарабарский» текст:

а) ш гухой ропалкымь ло лшоир улкашор пе жоцяк;

б) гко рохек лтафакь о передтой тсаллигелтой зисолозии рухгипа щеф нмонилти?

Задание 3. Расшифровать текст, созданный с помощью таблицы Виженера:

а) ыодхчаюъбькящячгчгщщб;

б) йсагофрем.

Задание 4. Расшифровать сообщения, зашифрованные методом постолбцовой транспозиции:

а) дбчргив ллуадпы яёвваон онсдгчо снтартс коввуии огасбнм ропеаеа;

б) бниен еоету зепдю рболв аррир саота стжеж уадлд днаьу.

Индивидуальные задания

1. Расшифровать криптограмму Цезаря (русский алфавит без *ё* и ъ).
2. Перевести текст с «тарабарской грамоты».
3. Расшифровать постолбцовый вариант маршрутной транспозиции.

Вариант 1

1. Ефвнгв злччиуирщлуципгв чцрнщлв ритуиуюерг.
2. Хифпь нметмалпа цшуря шебари – ифугепиер ракеракити и её нменоцашапиер.
3. Тояаи овпдт лррлн ьеиеа кмнжм.

Вариант 2

1. Рлыхс ри еиырс тсз оцрсб.
2. Паута лкапошикля ноцсиппой паутой ш кой лкенепи, ш татой носьфуекля ракеракигелтири рекоцари.
3. Сттлёбео тььпекс ыкешасни даченпиш икепыемь чпмотчос елбтентя саормен*.

Вариант 3

1. Лфхсулв цылх, ыхс рлнгнгв еогфхя ри дюегих еиырсм.
2. Паута щеф ракеракити – пе паута.
3. Ммауамр ычнчеуа пееттчд олпоаеу зооопме нвтноут аеозтос ёкмноня.

Вариант 4

1. Лфхсулыифнл тиуеюи еюдсую тусьол е Лцзии тул Тсрхлл Тлогхи.
2. Тшапкошый торньюкем шфсораек сющую лошмереппую тминкочмазигелтую лилкеру.
3. Сеяое лоддн утегн чклоы арате йыюоу нттвм ыиплы.

Вариант 5

1. Нултхсжугчлв угкугдгхюегих пихсзю кгэлхю лрчсупгщлл сх рифгрнщлсрлусегррсжс зсфхцтг.
2. Аццикишпая чмунна л цоноспикесьпой онемадией урпохепия, лшяфаппой ло лсохепиер фатопари цилкмищукишполки, пафышаекля тосьдор.
3. Сзветмт лаельае емлонял дыивазь оскеуан влоккна аягааия тмоесм* ьичсаа*.

Вариант 6

1. Хисулв ылфио фимыгф схрсфлхфв н угкувзц тулногзрюш ргцн.
2. Гер пешехелкшеппей гесошет, кер щосее оп ушемеп, гко илкипа у печо ш тамрапе.
3. Ундити миетьт нклевб еаёреы икнязт монедь ейотен юойсзи щпцянг иребад йелыче.

Вариант 7

1. Нгйзюм еютцфнрлн ДЖЦЛУ цеиуиррс еогзиих нсптябхиусп.
2. Пи оцип шекем пе щуцек нонукпыр цся томащся, токомый пе шывес иф чашапи.
3. Клшуе тслтр ояяро нртув ааьда узтнт чмооь иымв*.

Вариант 8

1. ПУХЛ – ецк хесим пиыхю.
2. Чмарр шоси шелик кяхесее, гер депкпем маллухцепия и ущехцепия.
3. Уоори мтрдт гпеца ирчее боиит нтймс еисия твеп*.

Вариант 9

1. Носз Ьиррср веовихфв сфрсестсосйрлнсп фсеуипиррсм кгэлхю лрчсупгщлл.
2. Рылсь ифмегеппая елкь сохь.
3. Хняде оезур ррард оыщнр шлиыу иутхг ечамо мшоаг аатно.

Вариант 10

1. Псрслз, ц нсхсусжс ефи аоипирхю сдугхлпю схрсфлхиоярс стуизиоиррсм е рип гожидуглыифнсм стиугщлл, ргкюегихфв жуцттсм.
2. Кьры пифтиж илкип пар цомохе пал шофшываюбий ощрап.
3. Ссхгй рлолц еедаа дпнзр иыоыь.

Вариант 11

1. Фхсмнсфхя нултхсфлфхипю УФГ сдцфосеоирг фосйрсфхяб еюылфоирлв чцрнщлл Амоиуг.
2. Елси оцип маф нохасеевь, гко пе лтафас, ко лко маф нохасеевь, гко пе нморосгас.
3. Жоьне еибег лдажо атвет юиела щсдащ еуёюи гдтщт.

Вариант 12

1. Гулчпихлнг нсоищ ногффсе еюыихсе оийлх е сфрсеи прсжлш фсеуипиррюш нултхсжугчлыифнлш флфхип.
2. Елси кы панмашисля т деси и лкапевь цомочою вшымякь тарпяри шо шлятую саюбюю лощату, ко пе цойцёвь цо пеё.
3. Удстщч тлтьеа еянтйс шныопт еехвоь нсианю ичмре* еаеис*.

Вариант 13

1. Зегзщгхлоихрлм тгулйфнлм фхцзирх Аегулфх Жгоцг кгосйло сфрсею фсеуипиррсм гожидую е ргыгои зиевхргзщгхсжс еинг.
2. Огепь лгалксишые сюци, машпо тат огепь пелгалкпые, оципатошо лтсоппы т гёмлкшолки.
3. Кгеме тотнд одсоо моягс нбтот оиога гвмоё оаунт.

Вариант 14

1. Злгжрсфхлнг зсфхлжог хгнлш цфтишсе, ыхс кзсусеюш обзим тугнхлыифнл ри сфхгосфя.

2. Гко шы цесаси шо шмеря кеммома? Я олкашасля хиш.

3. Суое рттл аьае зитг угьк длно.

Вариант 15

1. – Ифол обзим щирлхя тс угдсхи, хс осьгзя оцыьи обдсжс ыиосеинг, – жсегулего Гоинфим Пгнфлпселы Жсуянлм.

2. Жморой угис оцпопочочо нмычакь.

3. Киеуг антжл жьчау дятсб адоао яуемк смёаа валяя.

Лабораторная работа № 2
ТЕОРИЯ ЧИСЕЛ

Цель работы: получение основных сведений из курса теории чисел.

Необходимые теоретические сведения

Ниже рассматриваются: N – множество натуральных чисел, Z – множество целых чисел. Множество целых чисел Z – счетное, состоит из элементов 0; ±1; ±2; …; ± n; … . На нем определены две алгебраические операции – сложение и умножение. Эти операции обладают следующими свойствами (для любых $a,b,c \in Z$):

1) ассоциативность: $a+(b+c)=(a+b)+c$; $a\cdot(b\cdot c)=a\cdot(b\cdot c)$;

2) коммутативность: $b+a=a+b$; $a\cdot b=b\cdot a$;

3) существует нейтральный элемент – 0 и 1 соответственно:

$$a+0=0+a=a; \quad a\cdot 1=1\cdot a=a;$$

4) $(a+b)\cdot c=a\cdot c+b\cdot c$ – закон дистрибутивности;

5) для каждого целого $a \in Z$ существует единственное противоположное, то есть такое целое b, что $a + b = b + a = 0$.

Теорема 2.1 (*О делении с остатком*). Для любых целых чисел a и b, $b \neq 0$, существует единственные целые числа q и r $0 \le r < |b|$, такие, что $a = b \cdot q + r$.

В этом равенстве r называют остатком, а q – частным (неполным частным при $r \neq 0$) от деления a на b. При $r = 0$ величины b и q называют делителями или множителями числа a. Читатель со школьной скамьи умеет находить частное и остаток методом деления уголком.

Следствие. Пусть b – натуральное число, $b > 1$. Для всякого целого числа a и максимального целого $m \ge 0$ с условием $a > b^m$ существуют единственные целые a_i, $0 \le i < b$, такие, что $a = \pm\left(a_m b^m + a_{m-1} b^{m-1} + ... + a_0\right)$.

Такое равенство записывают сокращённо $a = \pm(a_m a_{m-1} \ldots a_0)_b$ или $a = \pm a_m a_{m-1} \ldots a_0$ (если b известно по контексту) и называют записью числа a в b-ичной позиционной системе счисления или системе счисления по основанию b.

Нам кажется естественной привычная десятичная позиционная система записи целых чисел $(b = 10)$. В различных ситуациях более удобными оказываются другие основания. К примеру, во всех компьютерах на микроуровне вычисления проводятся в двоичной системе счисления. Для перехода к ней с десятичной применяют промежуточную – 16-ричную систему счисления.

Лемма 2.1. Если в равенстве $a_1 + a_2 + \ldots + a_n = b_1 + b_2 + \ldots + b_m$ все слагаемые – целые числа и все, кроме может быть одного, делятся на целое d, то и это исключенное слагаемое делится на d.

Определение 2.1. Если целые числа $a_1, a_2, \ldots, a_n$ делятся на целое d, то d называют их *общим делителем*.

В дальнейшем речь идет только о положительных целых делителях.

Определение 2.2. Максимальный из общих делителей целых чисел $a_1, a_2, \ldots, a_n$ называется их *наибольшим общим делителем* и обозначается как НОД $(a_1, a_2, \ldots, a_n)$.

Теорема 2.2. Если $a = b \cdot q + c$, то НОД (a, b) = НОД (b, c).

Теорема 2.2 позволила Евклиду (примерно 2300 лет тому назад) обосновать следующий факт.

Теорема 2.3. Наибольший общий делитель целых чисел a и b $(a > b)$ равен последнему отличному от нуля остатку цепочки равенств:

$$a = b \cdot q_1 + r_1,$$

$$b = r_1 \cdot q_2 + r_2,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$r_{n-2} = r_{n-1} \cdot q_n + r_n,$$

$$r_{n-1} = r_n \cdot q_{n+1},$$

то есть r_n = НОД (a, b).

Теорема 2.3 формулирует второй способ вычисления наибольшего общего делителя по алгоритму Евклида: вычисляем последовательно разности $a-b=c,\ b-c=d,\ldots$ до получения последней ненулевой разности, которая и совпадает с НОД (*a*, *b*).

Пример 2.1. С помощью алгоритма Евклида найти НОД (72, 26).

Решение. В соответствии с теоремой 2.3 $72=26\cdot 2+20;\ \ 26=20\cdot 1+6;$ $20=6\cdot 3+2;\ 6=2\cdot 3$. Следовательно, НОД (72, 26) = 2.

Теорема 2.4. Если d = НОД (*a*, *b*), то существуют такие целые *u* и *v*, что выполняется следующее соотношение (Безу): $d=au+bv$.

Пример 2.2. Из примера 2.1 следует, что

$$2=20+6\cdot(-3)=20+\big(26+20\cdot(-1)\big)\cdot(-3)=20\cdot 4+26\cdot(-3)=$$
$$=\big(72+26\cdot(-2)\big)\cdot 4+26\cdot(-3)=72\cdot 4+26\cdot(-11).$$

Такой способ получения соотношения Безу для конкретных целых чисел называется *расширенным алгоритмом Евклида*. Он состоит из двух этапов:

1) собственно алгоритма Евклида – прогонки вниз;

2) прогонки вверх – последовательного выражения остатков в каждом из шагов предыдущего этапа (с соответствующим приведением подобных на каждом шаге).

Определение 2.3. Натуральное число $p>1$ называется *простым*, если оно делится только на 1 и на себя.

Теорема 2.5. Всякое натуральное число $n>1$ либо является простым числом, либо имеет простой делитель.

Заметим, что из соотношения $n=p\cdot q$ натуральных чисел, больших единицы, следует, что либо *p*, либо *q* принадлежит отрезку $[2;\sqrt{n}]$. Легко видеть, что наименьший натуральный делитель $p>1$ натурального числа $n>1$ является простым числом.

Исторически первый метод проверки натурального числа $n>1$ на простоту заключается в делении его на простые числа, не превосходящие $\sqrt{n}$, и называется

«*решето Эратосфена*». К настоящему времени разработан достаточно большой цикл алгоритмов проверки числа на простоту.

Теорема 2.6 (*Евклида*). Простых чисел бесконечно много.

Значение простых чисел в том, что они по теореме 2.5 являются составными кирпичиками всех натуральных чисел.

Определение 2.4. Целые числа a и b называются *взаимно простыми*, если НОД $(a, b)=1$.

Теорема 2.7 (*Критерий взаимной простоты целых чисел*). Целые числа a и b взаимно просты тогда и только тогда, когда существуют такие целые u и v, что выполняется равенство $a \cdot u + b \cdot v = 1$.

Следствие. НОД$(ac, b)=1$ тогда и только тогда, когда НОД $(a, b)=1$ и НОД $(c, b)=1$.

Важным в теории чисел и ее приложениях является следующее свойство взаимно простых целых чисел.

Лемма 2.2. Пусть произведение целых чисел ab делится на целое число c и НОД $(a, c)=1$. Тогда b делится на c.

Теорема 2.8 (*Основная теорема арифметики*). Всякое целое число $n>1$ однозначно раскладывается в произведение простых множителей

$$n = \pm p_1 \cdot p_2 \cdot \ldots \cdot p_s .$$

Если в этом равенстве собрать одинаковые множители, то получим каноническое разложение целого числа: $n = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \ p_t^{r_t}$.

Пример 2.3. Приведем примеры канонических разложений целых чисел:

а) $196 = 2 \cdot 98 = 2 \cdot 2 \cdot 49 = 2^2 \cdot 7^2$;

б) $2^{12} - 1 = 4095 = 3^2 \cdot 5 \cdot 7 \cdot 13$.

Теорема 2.9. Пусть m – натуральное число, $m>1$. Для любых целых чисел a и b следующие условия равносильны:

1) a *и* b *имеют одинаковые остатки от деления на* m;

2) $a-b$ *делится на* m, *то есть* $a-b=mq$ *для подходящего целого* q;

3) $a = b + mq$ *для некоторого целого* q.

Определение 2.5. Целые числа a и b называются *сравнимыми по модулю* m, если они удовлетворяют одному из условий теоремы 2.9. Этот факт обозначают формулой $a \equiv b (\mathrm{mod}\, m)$ или $a \equiv b (m)$ и называют данную формулу *сравнением*.

Пример 2.4. $-5 \equiv 7 (\mathrm{mod}\ 4) \equiv 11 (\mathrm{mod}\ 4) \equiv 23 (\mathrm{mod}\ 4) \equiv 3 (\mathrm{mod}\ 4)$.

Пример 2.5. Если $a = mq + r$, то $a \equiv r (\mathrm{mod}\, m)$ – всякое целое число сравнимо по модулю m со своим остатком от деления на m. Это следует из определения 2.5 и второго условия теоремы 2.9. Ведь $a - r$ делится на m.

Основные свойства сравнений

1. Пусть $a \equiv b (\mathrm{mod}\, m)$. Тогда $(a \pm c) \equiv (b \pm c) (\mathrm{mod}\, m)$ для всякого целого c, то есть к обеим частям сравнения можно добавить (или вычесть из обеих частей) одно и то же число.

2. Сравнения можно почленно складывать и вычитать: если $a \equiv b (\mathrm{mod}\, m)$, $c \equiv d (\mathrm{mod}\, m)$, то $(a + c) \equiv (b + d) (\mathrm{mod}\, m)$; $(a - c) \equiv (b - d) (\mathrm{mod}\, m)$.

3. Сравнения можно почленно перемножать: если $a \equiv b (\mathrm{mod}\, m)$ $c \equiv d (\mathrm{mod}\, m)$, то $ac \equiv bd (\mathrm{mod}\, m)$.

4. Сравнения можно почленно возводить в любую натуральную степень: если $a \equiv b (\mathrm{mod}\, m)$, то $a^n \equiv b^n (\mathrm{mod}\, m)$.

5. Если в сравнении $a \equiv b (\mathrm{mod}\, m)$ числа a, b, m имеют общий множитель d, то на него сравнение можно сократить: $a / d \equiv b / d (\mathrm{mod}\, m / d)$.

6. Сравнение можно сократить на общий множитель, взаимно простой с модулем: если $a = ad_1, b = db_1$, НОД (d, m) = 1, то из сравнения $da_1 \equiv db_1 (\mathrm{mod}\, m)$ следует сравнимость a_1 и b_1 по модулю m: $a_1 \equiv b_1 (\mathrm{mod}\, m)$.

7. Сравнение можно умножить на любой целый множитель: если $a \equiv b (\mathrm{mod}\, m)$, то $at \equiv bt (\mathrm{mod}\, m)$ для всякого целого t.

8. Рефлексивность: $a \equiv a \pmod m$ для любого целого a и всякого натурального m >1.

9. Симметричность: если $a \equiv b \pmod m$, то $b \equiv a \pmod m$.

10. Транзитивность: если $a \equiv b \pmod m$, $b \equiv c \pmod m$, то $a \equiv c \pmod m$.

Теорема 2.10 (*Малая теорема Ферма*). Пусть p – простое число, и целое число a не делится на p. Тогда $a^{p-1} \equiv 1 \pmod p$.

Теория сравнений и малая теорема Ферма позволяют быстро находить остаток от деления большого числа на простое число.

Пример 2.6. Найдем остаток от деления 39^{29} на 31.

Решение. $39 \equiv 8 \pmod{31}$. Поэтому в силу свойства 4 сравнений $39^2 \equiv 8^2 \pmod{31} \equiv 2 \pmod{31}$. Двоичная запись: $29 = 11101$. Следовательно, для любого натурального a величина $a^{29} = a^{2^4} \cdot a^{2^3} \cdot a^{2^2} \cdot a$. Далее, $39^4 \equiv 8^4 \pmod{31} \equiv 2^2 \pmod{31}$. Поэтому $39^8 \equiv (39^4)^2 \pmod{31} \equiv 4^2 \pmod{31}$. Тогда $39^{16} \equiv (39^8)^2 \pmod{31} \equiv 16^2 \pmod{31} \equiv 8 \pmod{31}$. Следовательно, $39^{29} \equiv 8 \cdot 16 \cdot 4 \cdot 8 \pmod{31} \equiv 4 \cdot 4 \cdot 8 \pmod{31} \equiv 4 \pmod{31}$. Таким образом, остаток от деления 39^{29} на 31 равен 4.

Задания для аудиторной работы

Задание 1. Найти канонические разложения чисел $a = 627, b = 399$.

Решение.

627	3	399	3
209	11	133	7
19	19	19	19
1		1	

Следовательно, $627 = 3 \cdot 11 \cdot 19, 399 = 3 \cdot 7 \cdot 19$.

Задание 2. Найти НОД (627, 399) пользуясь: а) алгоритмом Евклида, б) разложением чисел на простые множители.

Решение. Применим алгоритм Евклида.

$627 = 399 \cdot 1 + 228$; $399 = 228 \cdot 1 + 171$; $228 = 171 \cdot 1 + 57$; $171 = 57 \cdot 3$

Следовательно, НОД (627, 399) = 57.

Найдём НОД (*a, b*), воспользовавшись разложением на простые множители чисел *a* и *b*, полученным в решении предыдущего задания: $627 = \underline{3} \cdot 11 \cdot \underline{19}$; $399 = \underline{3} \cdot 7 \cdot \underline{19}$. Следовательно, наибольшим общим делителем будет произведение одинаковых множителей, входящих, как в одно, так и в другое разложения чисел: НОД (627, 399) $= \underline{3} \cdot \underline{19} = 57$.

Найдем НОД (*a, b*) методом вычитаний:

$627 - 399 = 228$; $399 - 228 = 171$; $228 - 171 = 57$; $171 - 57 = 114$;

$114 - 57 = 57$; $57 - 57 = 0$. Следовательно, НОД $(627, 399) = 57$.

Задание 3. С помощью расширенного алгоритма Евклида найти целые числа *u, v,* удовлетворяющие соотношению Безу: $au + bv = \text{НОД}\,(a, b)$ для целых чисел $a = 110, b = 48$.

Решение. Сначала найдем по алгоритму Евклида НОД (110, 48).

$110 = 48 \cdot 2 + 14$; $48 = 14 \cdot 3 + 6$; $14 = 6 \cdot 2 + 2$; $6 = 3 \cdot 2$.

Следовательно, НОД (110, 48) = 2.

Теперь построим соотношение Безу для данных *a* и *b*.

$110 = 48 \cdot 2 + 14$, поэтому $14 = 110 + 48 \cdot (-2)$;

$48 = 14 \cdot 3 + 6$, поэтому $6 = 48 + 14 \cdot (-3)$;

$14 = 6 \cdot 2 + 2$, поэтому $2 = 14 + 6 \cdot (-2)$.

В это равенство подставим выше полученное выражение для 6 и приведем подобные относительно чисел 48 и 14. Итак, $2 = 14 + 6 \cdot (-2) = 14 + (48 + 14 \cdot (-3))(-2) = 14 \cdot 7 + 48 \cdot (-2)$. В полученное

выражение для НОД (110, 48) = 2 подставим вышеприведенное выражение числа 14. Получим окончательно

$$2 = 14 \cdot 7 + 48 \cdot (-2) = (110 + 48 \cdot (-2))7 + 48 \cdot (-2) = 110 \cdot 7 + 48 \cdot (-16) = 2.$$

Задание 4.

а) Найти остаток от деления 2^{100} на 3.

Решение. 2 делится на 3 с остатком 2, 2^2 делится на 3 с остатком 1. При дальнейшем возведении двойки в степень остатки от деления будут чередоваться 2, 1, 2, 1, 2, … . Значит, в силу четности степени 100 остаток от деления требуемого числа на 3 будет равен 1.

2-й способ – методом сравнений, по аналогии с примером 2.6. $2^{100} = 4^{50} = (3+1)^{50} \equiv 1^{50} = 1.$

б) Найти остаток от деления $1989 \cdot 1990 \cdot 1991 + 1992^7$ на 7.

Решение. Заменим каждое число на его остаток от деления на 7:

_1989 | 7	_1990 | 7	1991 = 7 · 284 + 3;
14 | 284	14 | 284	
_58	_59	1992 = 7 · 284 + 4.
56	56	
_29	_30	
28	28	
1	2	

$1 \cdot 2 \cdot 3 + 4^3 = 6 + 64 = 70$. 70 : 7 = 10. Следовательно, остаток равен нулю.

в) Найти остаток от деления 9^{100} на 8.

Решение. Заменим 9 на его остаток 1 от деления на 8. Имеем $1^{100} = 1$. Значит, остаток от деления 9^{100} на 8 равен 1.

г) Найти остаток от деления 3^{1989} на 7.

Решение. 3 делится на 7 с остатком 3. 3^2 делится на 7 с остатком 2. Далее достаточно на 3 умножить только остаток и делать выводы. 3^3 делится на 7 с остатком 6, 3^4 делится на 7 с остатком 4, 3^5 делится на 7 с остатком 5, 3^6 делится на 7 с остатком 1, 3^7 делится на 7 с остатком 3. Получили один из предыдущих

остатков, значит «зациклились». Число 3^7 дает тот же остаток деления на 7, что и 3^1. Значит, длина цикла равна 6. $1989 = 331 \cdot 6 + 3$. Число 3^{1989} дает тот же остаток от деления на 7, что и 3^3, то есть 6.

Индивидуальные задания

1. Найти канонические разложения чисел a и b.

2. Найти НОД (a, b) пользуясь

а) алгоритмом Евклида,

б) разложением чисел на простые множители.

3. С помощью расширенного алгоритма Евклида найти целые u, v, удовлетворяющие соотношению Безу: $au + bv =$ НОД (a, b).

4. Найти остаток от деления данного числа на простое.

Вариант 1

1–3. a = 101398751, b = 326147777.

4. Найти остаток от деления 1998^{2001} на 29.

Вариант 2

1–3. a = 5999801, b = 48685811.

4. Найти остаток от деления 2005^{2003} на 17.

Вариант 3

1–3. a = 660422941, b = 36481301.

4. Найти остаток от деления 2001^{2005} на 17.

Вариант 4

1–3. a = 9002242397, b = 433817903.

4. Найти остаток от деления 2004^{2998} на 19.

Вариант 5

1–3. a = 9118515943, b = 3386496689.

4. Найти остаток от деления 1999^{2005} на 23.

Вариант 6

1–3. a = 5336161097, b = 196210799.

4. Найти остаток от деления 1998^{2001} на 19.

Вариант 7

1–3. a = 7049964661, b = 168687989.

4. Найти остаток от деления 1997^{2004} на 17.

Вариант 8

1–3. a = 83748733, b = 73435591.

4. Найти остаток от деления 1996^{2003} на 11.

Вариант 9

1–3. a = 16254559, b = 1029073.

4. Найти остаток от деления 2006^{1998} на 19.

Вариант 10

1–3. a = 6099377, b = 9568217.

4. Найти остаток от деления 2006^{1999} на 17.

Вариант 11

1–3. $a = 7957549$, $b = 23118553$.

4. Найти остаток от деления 2005^{1999} на 19.

Вариант 12

1–3. $a = 16088437$, $b = 18216949$.

4. Найти остаток от деления 1995^{2004} на 16.

Вариант 13

1–3. $a = 244604911$, $b = 61875907$.

4. Найти остаток от деления 2001^{1995} на 17.

Вариант 14

1–3. $a = 356216713$, $b = 31238065$.

4. Найти остаток от деления 2005^{2004} на 19.

Вариант 15

1–3. $a = 7409621$, $b = 6793883$.

4. Найти остаток от деления 2005^{2002} на 29.

Лабораторная работа № 3
КЛАССЫ ВЫЧЕТОВ

Цель работы: изучение классов вычетов, нахождение обратных элементов.

3.1. Необходимые теоретические сведения

При делении целых чисел на натуральное целое $m>1$ существует m различных остатков: 0, 1, 2, …, m – 1. Соответственно этим остаткам множество Z разбивается на m непересекающихся классов сравнимых друг с другом чисел, то есть имеющих один и тот же остаток от деления на m. В соответствии с остатками от деления на m эти классы будем обозначать через $\bar{0}, \bar{1}, ..., \overline{m-1}$. Таким образом, класс $\bar{i}=\{mq+i \mid q\in Z\}$ для каждого целого $i=0, 1, 2,..., m-1$. Любой представитель класса однозначно определяет свой класс: для каждого натурального числа $mq+i$ класс $\overline{mq+i}=\bar{i}$. Поскольку остаток – по-латински *residu* – переводится на русский как вычет, то множество всех классов по данному модулю сравнимых друг с другом чисел называют *множеством классов вычетов по модулю* и обозначают через Z/mZ. В силу сказанного $Z/mZ=\{\bar{0}, \bar{1}, ..., \overline{m-1}\}$ – множество из m элементов. Заметим, что для любых классов $\bar{k}, \bar{l}\in Z/mZ$ и для произвольных $k_1, k_2\in\bar{k}, l_1, l_2\in\bar{l}$ суммы k_1+l_1 и k_2+l_2 принадлежат одному классу из Z/mZ, так как эти суммы сравнимы друг с другом по модулю m согласно свойству 2 сравнений. Аналогично, произведения k_1l_1 и k_2l_2 лежат в одном классе из Z/mZ.

Определим операции сложения на Z/mZ. Полагаем суммой $\bar{k}\oplus\bar{l}$ такой единственный класс $\bar{z}$ из Z/mZ, в который попадают все суммы k_1+l_1 и k_2+l_2 для $k_1, k_2\in\bar{k}$, $l_1, l_2\in\bar{l}$, а произведением $\bar{k}\bar{l}$ – тот класс из Z/mZ, в который попадают произведения $\tilde{k}\tilde{l}$ для $\tilde{k}\in\bar{k}$, $\tilde{l}\in\bar{l}$.

Поскольку сложение и умножение в Z/mZ однозначно определяются умножением представителей классов, то свойства 1–5 операций сложения и умножения целых чисел справедливы и в Z/mZ.

1) $\bar{k} \oplus \bar{l} = \bar{l} \oplus \bar{k}$; $\bar{k}\bar{l} = \bar{l}\bar{k}$ – коммутативность;

2) $\bar{k} \oplus (\bar{l} \oplus \bar{r}) = (\bar{k} \oplus \bar{l}) \oplus \bar{r}$; $\bar{k}(\bar{l}\bar{r}) = (\bar{k}\bar{l})\bar{r}$ – ассоциативность;

3) существует нейтральный элемент: $\bar{k} \oplus \bar{0} = \bar{k}$; $\bar{k}\bar{1} = \bar{k}$;

4) для всякого $\bar{k} \in Z/mZ$ существует единственный класс $\bar{l}$, такой, что $\bar{k} \oplus \bar{l} = \bar{0}$, им является $\bar{l} = \overline{m-k}$;

5) $(\bar{k} \oplus \bar{l})\bar{r} = (\bar{k}\bar{r}) \oplus (\bar{l}\bar{r})$ – дистрибутивность.

Благодаря отмеченным свойствам операций сложения и умножения множество Z/mZ в алгебре относят к классу коммутативных колец с единицей и называют *кольцом классов вычетов по модулю m*.

Определение 3.1. Элемент $\bar{k} \in Z/mZ$ называется *обратимым*, если найдется такой класс $\bar{l} \in Z/mZ$, что $\bar{k}\bar{l} = \bar{1}$. Тогда класс $\bar{l}$ называют *обратным к классу* $\bar{k}$.

Из ассоциативности умножения в кольце Z/mZ вытекает, что если $\bar{k}$ – обратимый класс, то обратный класс определен однозначно.

Лемма 3.1. Пусть $\bar{k} \in Z/mZ$ такой класс, что НОД $(k, m) = 1$. Тогда:

1) для каждого $\bar{l} \neq \bar{0}$ произведение $\bar{k}\bar{l} \neq \bar{0}$;

2) $\bar{k}\bar{l_1} \neq \bar{k}\bar{l_2}$, если $\bar{l_1} \neq \bar{l_2}$;

3) отображение $f : \bar{x} \to \bar{k}\bar{x}$ инъективно и, следовательно, биективно на множестве Z/mZ (на множестве ненулевых элементов из Z/mZ);

4) $\bar{k}$ – обратимый класс в кольце Z/mZ.

Замечание. В условиях леммы 3.1 НОД $(k,m)=1$, поэтому, согласно критерию взаимной простоты целых чисел, существуют такие целые $u, v \in Z$, что $ku+mv=1$. Тогда $\bar{1}=\overline{ku}+\overline{mv}=\overline{ku}$. Следовательно, $\bar{u}$ – обратный к $\bar{k}$ класс.

Лемма 3.2. Пусть $\bar{k} \in Z/mZ$ – такой класс, что НОД $(k, m)=d>1$. Тогда

1) существует класс $\bar{l} \neq \bar{0}$, что $\overline{kl}=\bar{0}$;

2) существуют классы $\overline{l_1} \neq \overline{l_2}$ такие, что $\overline{kl_1}=\overline{kl_2}$;

3) для всех $\bar{l} \neq \bar{0}$ произведение $\overline{kl} \neq \bar{1}$, то есть класс $\bar{l}$ не обратим в кольце Z/mZ.

Теорема 3.1. Класс $\bar{k}$ из кольца Z/mZ обратим тогда и только тогда, когда НОД $(k, m)=1$. Если $m=p$ – простое число, то в кольце Z/mZ каждый ненулевой класс обратим. Обратный класс также обратим. Произведение обратимых классов есть обратимый класс.

Поскольку Z/mZ состоит из конечного множества элементов, то сложение и умножение можно задавать поэлементно в виде таблиц.

Пример 3.1. Напишем таблицы сложения и умножения в $Z/3Z$:

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

Из таблицы умножения непосредственно видно, что классы $\bar{1}$ и $\bar{2}$ обратны сами себе, то есть обратимы все ненулевые классы $Z/3Z$ в полном соответствии с теоремой 3.1.

Определение 3.2. *Функция Эйлера* – функция натурального аргумента $\varphi(m)$, которая каждому натуральному числу $m>1$ ставит в соответствие количество натуральных чисел, меньших m и взаимно простых с m.

Перечислим ***основные мультипликативные свойства функции Эйлера*:**

1. $\varphi(p)=p-1$ для каждого простого числа p.

2. $\varphi(p^n)=p^n-p^{n-1}$ для каждого простого числа p и для произвольного натурального $n\geq 1$.

3. Если НОД $(n, m)=1$, то $\varphi(nm)=\varphi(n)\varphi(m)$.

4. Если $n=p_1^{k_1}p_2^{k_2}...p_s^{k_s}$ – каноническое разложение числа m, то $\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_s}\right)$.

Пример 3.2. Вычислим $\varphi(48)$. Поскольку $48=3\cdot 2^4$, то согласно свойству 4 значение $\varphi(48)=48\cdot\left(1-\frac{1}{3}\right)\cdot\left(1-\frac{1}{2}\right)=16$.

Пример 3.3. Из теоремы 3.1 следует, что в кольце Z/mZ имеется в точности $\varphi(m)$ обратимых классов. Например, $\varphi(12)=4$. Значит, в кольце $Z/12Z$ имеется именно 4 обратимых элемента. Непосредственная проверка показывает, что этими классами являются $\bar{1}, \bar{5}, \bar{7}, \bar{11}$.

Теорема 3.2 (*Эйлера*). Если для целого числа a и натурального m НОД $(a, m)=1$, то $a^{\varphi(m)}\equiv 1(\mathrm{mod}\, m)$.

Алгебраическим сравнением n-й степени с одной неизвестной называется сравнение вида

$$a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 x^0 \equiv 0(\mathrm{mod}\, m),$$

где $a_n,\ a_{n-1},...,\ a_0 \in Z,\ n\in N,\ a_n \neq 0(\mathrm{mod}\, m)$.

Если при подстановке вместо x числа x_0 получается верное числовое сравнение, то x_0 называется *решением данного сравнения*. При этом и любое целое число вида $x_0 + mt$ также будет решением данного сравнения. Поэтому решением алгебраического сравнения можно считать класс вычетов $\overline{x_0}$. Универсальным способом решения алгебраических сравнений является испытание полной системы вычетов по модулю m, то есть целых чисел 0, 1, 2, …, $m-1$. Сравнение будет иметь столько решений, сколько вычетов полной системы ему удовлетворяют.

Пример 3.4. Решить сравнение $x^5 + x + 1 \equiv 0 (\mathrm{mod}\, 7)$.

Решение. Среди чисел 0, 1, 2, 3, 4, 5, 6 полной системы вычетов по модулю 7 удовлетворяют данному сравнению только два числа $x = 2$, $x = 4$. Поэтому указанное сравнение имеет два решения: $x \equiv 2 (\mathrm{mod}\, 7)$, $x \equiv 4 (\mathrm{mod}\, 7)$.

При решении сравнений часто используют преобразования, приводящие к равносильным сравнениям.

Задания для аудиторной работы

Задание 1. Вычислить $\varphi(n)$ для всех натуральных n от 2 до 12.

Задание 2. Вычислить $\varphi(60)$, $\varphi(81)$, $\varphi(89)$, $\varphi(2017)$, $\varphi(2018)$.

Решение. $60 = \underset{p_1}{2}^{2} \cdot \underset{p_2}{3} \cdot \underset{p_3}{5}$. Согласно свойству 4 функции Эйлера

$$\varphi(60) = 60\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 60 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 2 \cdot 2 \cdot 4 = 16.$$

$81 = 3^4$. Поэтому, согласно свойству 2 функции Эйлера:

$$\varphi(81) = 3^4 - 3^{3-1} = 3^4 - 3^3 = 81 - 27 = 54.$$

$\sqrt{89} < 10$; 89 не делится на все простые 2, 3, 5, 7, меньшие 10. Следовательно, 89 – число простое. Поэтому $\varphi(89) = 88$.

Задание 3. В кольцах $Z/5Z$ и $Z/6Z$ и составить таблицы сложения и умножения. Найти в этих кольцах пары взаимно обратных по умножению элементов. Указать количество таких пар и сравнить это количество с $\varphi(5)$ и $\varphi(6)$ соответственно.

Задание 4. В кольце классов вычетов по модулю 15 к каждому обратимому элементу найти обратный элемент.

Решение. Согласно теореме 2.1 в кольце $Z/15Z$ имеется $\varphi(15)=8$ классов вычетов, взаимно простых с модулем $m=15$. Эти классы составляют множество $G=\{\bar{1},\bar{2},\bar{4},\bar{7},\bar{8},\overline{11},\overline{13},\overline{14}\}$.

На языке сравнений равенство $\bar{a}\cdot\bar{x}=\bar{1}$ для $\bar{a}\in G$ выглядит как $ax\equiv 1(\mathrm{mod}\,15)$, а из теоремы Эйлера следует, что $a^8\equiv 1(\mathrm{mod}15)$. Умножив сравнение $ax\equiv 1(\mathrm{mod}\,15)$ на a^7, получим $x\equiv a^7(\mathrm{mod}15)$ согласно свойствам сравнений. Последовательно вычисляем

$$2^7=8\cdot 16\equiv 8(\mathrm{mod}\,15),\ \text{значит}\ (\bar{2})^{-1}=\bar{8};$$

$$4^7=16^3\cdot 4\equiv 4(\mathrm{mod}\,15),\ \text{значит}\ (\bar{4})^{-1}=\bar{4};$$

$$7^7=49^3\cdot 7\equiv 4^3\cdot 7\equiv 13,\ (\bar{7})^{-1}\equiv 1\bar{3};$$

$$11^7=121^3\cdot 11=1^3\cdot 11\equiv 11(\mathrm{mod}15),\ (\overline{11})^{-1}=11;$$

$$14^7=2^7\cdot 7^7\equiv 8\cdot 13(\mathrm{mod}15)\equiv(-7)\cdot(-2)(\mathrm{mod}15)=14(\mathrm{mod}15),\ (\overline{14})^{-1}=\overline{14}.$$

Задание 5. В кольце $Z/2005Z$ найти обратные к элементам $\bar{5},\ \bar{6},\ \bar{7}$.

Решение.

1. Находим $\varphi(2005)$:

$$2005=5\cdot 401;\ \varphi(2005)=2005\left(1-\frac{1}{5}\right)\left(1-\frac{1}{401}\right)=1600.$$

2. Находим в кольце $Z/2005Z$ обратные к элементам: а) $\bar{5}$; б) $\bar{6}$; в) $\bar{7}$.

а) НОД $(2005; 5)=5 \Rightarrow \overline{5}^{-1}$ не обратим.

б) НОД $(2005; 6)=1 \Rightarrow \overline{6}^{-1}$ обратим.

$$2005 = 6 \cdot 334 + 1;$$

$$1 = 6 - 5 \cdot 1 = 6 - 5(2005 + 6(-334)) = 6 - 5 \cdot 2005 + 5 \cdot 6 \cdot 334 = -5 \cdot 2005 + 6 \cdot 1671;$$

$$\overline{6}^{-1} = \overline{1671}.$$

в) НОД $(2005; 7)=1 \Rightarrow \overline{7}^{-1}$ обратим;

$$2005 = 7 \cdot 286 + 3;\ 1 = 7 - 2 \cdot 3 = 7 - 2(2005 + 7(-286)) = -2 \cdot 2005 + 573 \cdot 7.$$

$$\overline{7}^{-1} = \overline{573}.$$

Индивидуальные задания

1. Построить таблицы сложения и умножения в кольце: а) Z/kZ; б) Z/nZ.

2. Вычислить $\varphi(k)$, $\varphi(n)$ (k, n – из первого задания), $\varphi(m)$ (m – из четвертого задания).

3. В кольцах Z/kZ, Z/nZ (первое задание) найти пары взаимно обратных по умножению элементов.

4. В кольце Z/mZ найти обратные к элементам $\overline{5}, \overline{6}, \overline{7}$.

5. Решить кубическое сравнение.

Вариант 1

1. $k=11;$ $n=24.$ 4. $m=2001.$ 5. $132x^3+143x^2+23x-19 \equiv 5 (\mathrm{mod} 11).$

Вариант 2

1. $k=13;$ $n=18.$ 4. $m=2002.$ 5. $169x^3+143x^2+23x-19 \equiv 5 (\mathrm{mod} 13).$

Вариант 3

1. $k=11;$ $n=23.$ 4. $m=2000.$ 5. $253x^3+46x^2+29x-49 \equiv 5 (\mathrm{mod}\, 23).$

Вариант 4

1. $k=17;$ $n=21.$ 4. $m=2003.$ 5. $187x^3+34x^2+23x-19\equiv 5(\mathrm{mod}17).$

Вариант 5

1. $k=19;$ $n=26.$ 4. $m=2004.$ 5. $132x^3+143x^2+23x-19\equiv 5(\mathrm{mod}11).$

Вариант 6

1. $k=13;$ $n=27.$ 4. $m=2005.$ 5. $117x^3+143x^2+3x-19\equiv 5(\mathrm{mod}13).$

Вариант 7

1. $k=17;$ $n=28.$ 4. $m=2006.$ 5. $63x^3+154x^2+23x-19\equiv 5(\mathrm{mod}7).$

Вариант 8

1. $k=12;$ $n=29.$ 4. $m=2007.$ 5. $319x^3+145x^2+23x-19\equiv 5(\mathrm{mod}29).$

Вариант 9

1. $k=15;$ $n=23.$ 4. $m=2008.$ 5. $253x^3+115x^2+12x-9\equiv 5(\mathrm{mod}23).$

Вариант 10

1. $k=14;$ $n=31.$ 4. $m=2009.$ 5. $341x^3+155x^2+23x-19\equiv 5(\mathrm{mod}31).$

Вариант 11

1. $k=17;$ $n=30.$ 4. $m=2010.$ 5. $85x^3+204x^2+13x-19\equiv 5(\mathrm{mod}17).$

Вариант 12

1. $k=9;$ $n=29.$ 4. $m=2011.$ 5. $145x^3+348x^2+23x-17\equiv 5(\mathrm{mod}29).$

Вариант 13

1. $k=17$; $n=22$. 4. $m=2012$. 5. $153x^3+187x^2+11x-9\equiv 5(\mathrm{mod}17)$.

Вариант 14

1. $k=19$; $n=14$. 4. $m=2013$. 5. $361x^3+209x^2+23x-11\equiv 5(\mathrm{mod}19)$.

Вариант 15

1. $k=16$; $n=23$. 4. $m=2014$. 5. $95x^3+228x^2+23x-9\equiv 5(\mathrm{mod}19)$.

Лабораторная работа № 4
ГРУППЫ И ПОДГРУППЫ

Цель работы: получение основных сведений о группах и подгруппах.

Необходимые теоретические сведения

Группы

Определение 4.1. *Группой* называется непустое множество G с одной определенной на нем бинарной алгебраической операцией, относительно которой выполняются следующие свойства:

1) ассоциативность: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ для любых $a, b, c \in G$;

2) существует нейтральный элемент (единица), то есть такой элемент $e \in G$, что $g \cdot e = e \cdot g = g$ для каждого $g \in G$;

3) каждый элемент $g \in G$ имеет обратный, то есть такой элемент $h \in G$, что $g \cdot h = h \cdot g = e$ (в этом случае пишут: $h = g^{-1}$).

Группы делятся на конечные и бесконечные по числу элементов, на *коммутативные* и *некоммутативные* в соответствии со следующим определением.

Определение 4.2. Группа G называется *коммутативной*, или *абелевой*, если определенная в ней операция обладает свойством

4) $ab = ba$ для всех $a, b \in G$.

Определение 4.3. *Порядком конечной группы* G называется количество элементов этой группы и обозначается $|G|$.

По исторической традиции все аддитивные группы (с операцией сложения) относятся к классу коммутативных групп. Для каждого натурального n найдется коммутативная конечная группа порядка n. Например, $(Z/nZ, +)$.

Теорема 4.1. Пусть a – фиксированный элемент произвольной группы G. Пусть $\langle a\rangle = \{a^0 = e, a, a^2, ..., a^{-1}, a^{-2}, ...\}$ – множество всевозможных степеней элемента а. Тогда $\langle a\rangle$ – группа, причём абелева.

Определение 4.4. Группа $\langle a\rangle$ из теоремы 4.1 называется *циклической группой*, порожденной элементом a.

Теорема 4.2. Пусть элемент $a \in G$ обладает свойством: $a^n = e$ для некоторого целого n и $a^k \neq e$ для всех целых k, $1 \le k < n$. Тогда циклическая группа $\langle a\rangle$ имеет порядок n и $\langle a\rangle = \{a, a^2, ..., a^n = e\}$.

Определение 4.5. Величина n из теоремы 4.2 называется *порядком элемента* $a \in G$. Если же для элемента $a \in G$ такого n не существует, то говорят, что элемент $a \in G$ имеет *бесконечный порядок*.

Из определения циклической группы следует, что она абелева, содержит счетное или конечное множество элементов и во втором случае имеет четкую структуру, выражаемую теоремой 4.2.

Теорема 4.3. Для каждого простого числа p множество всех ненулевых классов из кольца классов вычетов Z/nZ образует группу Z/pZ^* относительно операции умножения, причем эта группа является циклической.

Пусть Ω – конечное множество из n элементов. Поскольку природа его элементов для нас не существенна, удобно считать, что $\Omega = \{1, 2, ..., n\}$.

Определение 4.6. Всякая биекция, то есть взаимно однозначное отображение Ω в себя, называется *подстановкой* на Ω.

Подстановку $f : i \to f(i),\ i = 1, 2, ..., n$, удобно изображать в развернутой и наглядной форме в виде двустрочной таблицы:

$$f = \begin{pmatrix} 1 & 2 & ... & n \\ f(1) & f(2) & ... & f(n) \end{pmatrix}.$$

В этой таблице каждый i-й столбец четко указывает, в какой элемент $f(i)$ преобразуется элемент i, $1 \le i \le n$. Подстановки перемножаются в соответствии с общим правилом композиции отображений: $(gf)(i) = g(f(i))$. Чаще всего

$gf \neq fg$, то есть композиция подстановок не обладает свойством коммутативности. Очевидно, тождественная подстановка $e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$ играет роль единицы относительно композиции подстановок. Как известно, композиция отображений является ассоциативной операцией, поэтому и композиция подстановок ассоциативна. Каждая подстановка – обратимая операция. Чтобы найти для подстановки f обратную подстановку f^{-1} достаточно в таблице $f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$ переставить строки местами, а затем столбцы *упорядочить по возрастанию элементов* первой строки.

Таким образом, подстановки на Ω образуют группу относительно операции композиции отображений – умножения подстановок. Ее называют симметрической группой на n элементах и обозначают через S_n.

Теорема 4.4. Порядок группы S_n равен $n!$.

Пусть f – произвольная подстановка из S_n. Из двустрочной таблицы, задающей f, выбросим столбцы с одинаковыми элементами.

Определение 4.7. *Циклом* длиной k называется подстановка вида

$$f_k = \left(i, f(i), \dots, f^{t_k - 1}(i)\right) = \begin{pmatrix} i & f(i) & \dots & f^{t_k - 1}(i) \\ f(i) & f^2(i) & \dots & i \end{pmatrix}.$$

Цикл длиной 2 называется *транспозицией.* Циклы без общих элементов называются *независимыми*, или *непересекающимися.*

Теорема 4.5. Каждая подстановка $f \in S_n$, $f \neq l$, является произведением независимых циклов длиной $l \geq 2$. Это разложение в произведение определено однозначно с точностью до порядка следования циклов.

Теорема 4.6. Каждая подстановка $f \in S_n$ раскладывается в произведение транспозиций. Любые два разложения данной подстановки в произведения транспозиций содержат либо четное число сомножителей, либо нечетное.

Пример 4.1. Разложить в произведение циклов и транспозиций подстановку

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 5 & 3 & 1 & 7 & 9 & 6 & 8 \end{pmatrix}.$$

Решение.

$$g = (1 \quad 2 \quad 4 \quad 3 \quad 5)(6 \quad 7 \quad 9 \quad 8) =$$

$$= (1 \quad 5)(1 \quad 3)(1 \quad 4)(1 \quad 2)(6 \quad 8)(6 \quad 9)(6 \quad 7).$$

Разложение подстановки в произведение транспозиций неоднозначно. К примеру, вышеприведенную подстановку можно представить в виде иного произведения транспозиций:

$$g = (1 \quad 2 \quad 4 \quad 3 \quad 5)(6 \quad 7 \quad 9 \quad 8) =$$

$$= (1 \quad 5)(1 \quad 3)(1 \quad 4)(1 \quad 2)(6 \quad 8)(3 \quad 4)(6 \quad 9)(3 \quad 4)(6 \quad 7)$$

Определение 4.8. Подстановка f называется *четной (нечетной)*, если ее разложение в произведение транспозиций содержит четное (нечетное) количество сомножителей.

Подгруппы

Определение 4.9. *Подгруппой* в группе $(G, \cdot)$ называется всякое непустое подмножество H элементов множества G, которое в свою очередь является группой относительно той же операции.

Теорема 4.7 (Критерий подгруппы). Непустое подмножество H группы $(G, \cdot)$ является подгруппой тогда и только тогда, когда для произвольных элементов $a, b \in H$ имеет место включение $a \cdot b^{-1} \in H$.

Определение 4.10. Подгруппа H группы G называется *собственной*, если $H \neq G$ и $H \neq \{e\}$.

Теорема 4.8. Всякая подгруппа циклической группы является циклической.

Теорема 4.9. Для каждого простого числа p мультипликативная группа Z/pZ^* содержит $p-1$ элементов и является циклической.

Определение 4.11. Пусть H – собственная подгруппа группы $(G, \cdot)$. Пусть $a \in G$. Через aH обозначим множество элементов $\{ah \mid h \in H\}$ и назовем его *левым смежным классом* группы G по подгруппе H.

Если существует $b \in G$, $b \notin H \cup aH$, можно построить новый левый смежный класс bH и так далее.

Аналогично строят правые смежные классы. Если каждый левый смежный класс совпадает с правым: $aH = Ha$, то тогда смежные классы называют *двусторонними*. Такими являются смежные классы в любой абелевой группе G.

Смежные классы обладают рядом важных свойств.

Теорема 4.10. Пусть H – собственная подгруппа группы G. Тогда:

1) каждый элемент $g \in G$ принадлежит какому-нибудь левому смежному классу по подгруппе H;

2) два элемента $a, b \in G$ принадлежат одному левому смежному классу тогда и только тогда, когда $a^{-1} \cdot b \in H$;

3) любые два левых смежных класса либо не пересекаются, либо совпадают;

4) для всякого $a \in G$ мощности множеств aH и H совпадают;

5) G есть объединение попарно непересекающихся левых (правых) смежных классов по подгруппе H;

6) мощности множеств всех левых и соответственно правых смежных классов группы G по подгруппе H равны.

Определение 4.12. *Индексом подгруппы H* в группе G называется мощность множества всех смежных классов группы G по данной подгруппе и обозначается через $|G : H|$.

Теорема 4.11 (*Лагранжа*). Порядок конечной группы делится на порядок любой ее подгруппы.

Следствие 4.1. В конечной группе индекс подгруппы равен частному от деления порядка группы на порядок подгруппы.

Следствие 4.2. Любая группа простого порядка является циклической и не содержит собственных подгрупп.

Следствие 4.3. Если G – конечная группа из n элементов, то для каждого $a \in G$ выполняется $a^n = e$. Другими словами, в конечной группе порядок любого ее элемента делит порядок самой группы.

Задания для аудиторной работы

Задание 1. Определить, является ли группой относительно операции умножения множество $\widetilde{C}$ всех комплексных чисел, имеющих единичный модуль.

Решение.

1) $z_1 \cdot (z_2 \cdot z_3) = (z_1 \cdot z_2) \cdot z_3$ для любых комплексных чисел;

2) нейтральный элемент $e = 1$: $z \cdot 1 = 1 \cdot z = z$ для любого комплексного числа;

3) для каждого $z = x + iy \in \widetilde{C}$ по условию $|z| = \sqrt{x^2 + y^2} = 1$, то есть $x^2 + y^2 = 1$; поэтому обратным элементом для $z = x + iy \in \widetilde{C}$ будет число $\bar{z} = x - iy$:

$$z \cdot \bar{z} = (x + iy) \cdot (x - iy) = z \cdot \bar{z} = (x - iy) \cdot (x + iy) = x^2 + y^2 = 1.$$

Следовательно, $\widetilde{C}$ – действительно группа.

Задание 2. Выяснить, является ли группой множество всех положительных вещественных чисел с бинарной алгебраической операцией возведения в степень?

Решение. Нет, потому что данная операция не ассоциативна. Например, $\left(2^3\right)^4 = 2^{12}$; а $2^{(3^4)} = 2^{81}$.

Задание 3. Разложить в произведение циклов и транспозиций подстановку

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 4 & 3 & 1 & 6 & 5 & 2 \end{pmatrix}.$$

Определить четность f.

Решение. Подстановка f перемещает 1 в 7, 7 в 2, 2 в 4, 4 в 1. В соответствии с определением 4.7 подстановка, действующая на элементы 1, 7, 2, 4 по данному правилу, а на все остальные – тождественно, называется циклом длиной 4. В соответствии с определением 4.7 данный цикл кратко записывают так: (1 7 2 4). Также f перемещает 3 в 3, 5 в 6 и 6 в 5. Так что запись $f = (1\,7\,2\,4)(3)(5\,6)$ указывает на то, как f перемещает элементы множества $\{1, 2, 3, 4, 5, 6, 7\}$. Поскольку цикл, состоящий из одного элемента, совпадает с тождественной подстановкой, то его при записи обычно опускают, т. е. $f = (1\,7\,2\,4)(5\,6)$ – произведение циклов. Отсюда получаем разложение подстановки f – произведение транспозиций:

$$f = (1\,4)(1\,2)(1\,7)(5\,6).$$

Как видим, f – четная подстановка.

Задание 4. Выписать циклическую группу, порожденную подстановкой

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 2 & 1 & 7 & 4 \end{pmatrix}.$$

Решение.

$$f^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 1 & 6 & 3 & 4 & 2 \end{pmatrix}; \qquad f^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 4 & 3 & 7 & 5 & 2 & 6 \end{pmatrix};$$

$$f^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 1 & 6 & 7 \end{pmatrix}; \qquad f^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 1 & 2 & 3 & 7 & 4 \end{pmatrix};$$

$$f^6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 7 & 3 & 6 & 5 & 4 & 2 \end{pmatrix}; \qquad f^7 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 7 & 1 & 2 & 6 \end{pmatrix};$$

$$f^8 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 1 & 4 & 3 & 6 & 7 \end{pmatrix}; \qquad f^9 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 6 & 3 & 2 & 5 & 7 & 4 \end{pmatrix};$$

$$f^{10}=\begin{pmatrix}1&2&3&4&5&6&7\\3&7&5&6&1&4&2\end{pmatrix};\qquad f^{11}=\begin{pmatrix}1&2&3&4&5&6&7\\5&4&1&7&3&2&6\end{pmatrix};$$

$$f^{12}=\begin{pmatrix}1&2&3&4&5&6&7\\1&2&3&4&5&6&7\end{pmatrix}=e.$$

Группа $\langle f\rangle$ – порядка 12.

Задание 5. Выяснить, обратима ли матрица $A=\begin{pmatrix}1&0&0\\0&1&0\\0&1&1\end{pmatrix}$ с элементами из кольца классов вычетов $Z/2Z$.

Решение. Найдем определитель матрицы A: $\det A=1\neq 0$. Следовательно, матрица A обратима.

Задание 6. Выписать циклическую группу, порожденную матрицей из предыдущего задания и указать ее порядок.

Решение. $A^2=\begin{pmatrix}1&0&0\\0&1&0\\0&1&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&0\\0&1&1\end{pmatrix}=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}=E$. Следовательно,

$\langle A\rangle=\{A,\ A^2=E\}$ – группа порядка 2.

Задание 7. Привести примеры подгрупп в группе $(Z,+)$. Образуют ли подгруппу:

а) все отрицательные числа; все положительные числа;

б) все четные числа; все нечетные числа;

в) множество целых чисел от 0 до 10; от –5 до 5;

д) все целые числа, делящиеся на 2007;

е) все целые числа с остатком 1999 при делении на 2007?

Задание 8. В любой группе имеются циклические подгруппы (иногда совпадающие с самой группой). А при каких условиях в группе имеются нециклические подгруппы? Привести примеры.

Задание 9. Показать, что мультипликативная группа $Z/8Z^*$ абелева, но не циклична, а $Z/9Z^*$ циклична.

Задание 10. Пусть $G = M_{1\times 4}(Z/2Z)$ – множество всевозможных строк-матриц с четырьмя координатами из $Z/2Z$ – группа относительно операции покоординатного сложения по модулю два. Сколько в этой группе элементов? Пусть H – следующее подмножество элементов группы G: $\left\{\underbrace{(0\ \ 0\ \ 0\ \ 0)}_{\bar{0}}, \underbrace{(1\ \ 0\ \ 1\ \ 1)}_{\bar{e}_1}, \underbrace{(0\ \ 1\ \ 0\ \ 1)}_{\bar{e}_2}, \underbrace{(1\ \ 1\ \ 1\ \ 0)}_{\bar{e}_1\cdot\bar{e}_2}\right\}$, здесь $\bar{0}=0,\ \bar{1}=1$.

Убедиться, что H – подгруппа, выписать таблицу смежных классов группы G по H.

Решение.

1. Поскольку каждая из координат может независимо от других принимать лишь два значения, то мощность группы G равна 16.

2. Уже неоднократно обсуждалось, что операция покоординатного сложения по модулю два ассоциативна. Составив таблицу сложения элементов множества H, можно убедиться, что сложение этих элементов не выводит за пределы H, то есть H замкнута относительно сложения. H содержит нейтральный элемент – нулевой вектор. Каждый вектор из H обратен самому себе. Таким образом, H удовлетворяет всем аксиомам из определения группы. Следовательно, H – подгруппа группы G.

3. Выпишем таблицу всех смежных классов группы G по подгруппе H.

	Класс $a+H$	$\bar{a}+0$	$\bar{a}+\bar{e}_1$	$\bar{a}+\bar{e}_2$	$a+(\bar{e}_1+\bar{e}_2)$
1	$\bar{0}+H=H$	(0000)	(1011)	(0101)	(1110)
2	$(1000)+H$	(1000)	(0011)	(1101)	(0110)
3	$(0100)+H$	(0100)	(1111)	(1001)	(1010)
4	$(0010)+H$	(0010)	(1001)	(0111)	(1100)

Задание 11. Выписать все элементы мультипликативной группы $(Z/36Z)^*$ сравнить их число с $\varphi(36)$. Выяснить, является ли эта группа циклической. Выписать таблицу смежных классов $(Z/36Z)^*/\langle 25\rangle$ группы $(Z/36Z)^*$ по циклической подгруппе $\langle 25\rangle$.

Решение. $G=(Z/36Z)^*=\{1,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 25,\ 29,\ 31,\ 35\}$, $\varphi(36)=$ $=\varphi(2^2\cdot 3^2)=12$. Группа G циклична, если в ней найдется элемент порядка $|G|$. То есть группа, порожденная им, совпадает со всей группой G. Попытаемся найти такой элемент. Наудачу выпишем циклическую подгруппу $\langle 5\rangle$: $\langle 5\rangle=\{5,\ 25,\ 5^3=17,\ 5^4=17\cdot 5=13,\ 5^5=13\cdot 5=29,\ 5^6=29\cdot 5=1\}$ – подгруппа порядка 6. По теореме Лагранжа все остальные элементы этой подгруппы имеют порядки, являющиеся делителями 6:

$\langle 7\rangle=\{7,\ 7^2=13,\ 7^3=13\cdot 7=19,\ 7^4=19\cdot 7=25,\ 7^5=25\cdot 7=31,\ 7^6=31\cdot 7=1\}$ – подгруппа порядка 6. Следовательно, ее элементы 7, 19, 31, не принадлежащие $\langle 5\rangle$, также имеют порядок, не превышающий 6:

$$\langle 11\rangle=\{11,\ 11^2=13,\ 11^3=13\cdot 11=35,\ 11^4=11\cdot 35=25,$$
$$11^5=25\cdot 11=23,\ 11^6=23\cdot 11=1\}-$$

подгруппа порядка 6. Следовательно, ее элементы 11, 23, 35, не принадлежащие подгруппам $\langle 7\rangle$ и $\langle 5\rangle$, также имеют порядок, не превышающий 6. Таким образом, все 12 элементов группы G имеют порядок, не превосходящий 6. Поэтому группа

G не может быть циклической. Множество $H = \langle 25 \rangle = \{25, 13, 1\}$ – подгруппа из трех элементов. Поэтому таблица смежных классов $(Z/36Z)^*/\langle 25 \rangle$ должна состоять из $12:3=4$ смежных классов. Одним из них всегда является подгруппа H. Вот оставшиеся три смежных класса:
$5H = \{5 \cdot 25 = 17,\ 5 \cdot 13 = 29,\ 5\};\ 7H = \{7 \cdot 25 = 31, 7 \cdot 13 = 19, 7\};$
$11H = \{11 \cdot 25 = 23,\ 11 \cdot 13 = 35,\ 11\}.$

Задание 12. Содержит ли группа $(Z/36Z)^*$ нециклическую подгруппу?

Решение. Да, содержит. В этой группе имеются три элемента второго порядка: 17, 19, 35. Эти элементы обратны сами себе, так как из условия $a^2 = e$ следует, что $a^{-1} = a$. Вместе с 1 они образуют замкнутую систему относительно умножения по модулю 36 и, в силу сказанного, нециклическую подгруппу из четырех элементов.

Индивидуальные задания

1. Выяснить, является ли группой множество … с операцией ….
2. Выписать циклическую группу $\langle f \rangle$. Указать ее порядок.
3. Выписать циклическую группу $\langle B \rangle$. Указать ее порядок.

Вариант 1

1. Множество целых чисел с операцией вычитания.
2. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 9 & 5 & 6 & 8 & 4 & 1 & 3 & 7 \end{pmatrix}$.
3. $B = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$.
4. Выписать все элементы мультипликативной группы кольца:

а) $Z/17Z$;

б) $Z/32Z$.

Сравнить количество этих элементов с $\varphi(17)$ и $\varphi(32)$ соответственно.

Является ли эта группа относительно умножения циклической?

Вариант 2

1. Множество всех положительных вещественных чисел с операцией деления.

2. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 9 & 1 & 7 & 8 & 5 & 2 & 4 \end{pmatrix}$.

3. $B = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$.

4. Выписать все элементы мультипликативной группы кольца:

а) $Z/19Z$;

б) $Z/30Z$.

Сравнить количество этих элементов с $\varphi(19)$ и $\varphi(30)$ соответственно.

Является ли эта группа относительно умножения циклической?

Вариант 3

1. Множество целых чисел с операцией $m * n = mn + m$.

2. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 9 & 8 & 3 & 1 & 4 & 2 & 6 & 7 \end{pmatrix}$.

3. $B = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}$.

4. Выписать все элементы мультипликативной группы кольца:

а) $Z/13Z$;

б) $Z/34Z$.

Сравнить количество этих элементов с $\varphi(13)$ и $\varphi(34)$ соответственно.

Является ли эта группа относительно умножения циклической?

Вариант 4

1. Множество целых чисел с операцией $m * n = m + 2n$.

2. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 6 & 2 & 8 & 1 & 3 & 4 & 7 & 5 \end{pmatrix}$.

3. $B = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$.

4. Выписать все элементы мультипликативной группы кольца:

а) $Z/11Z$;

б) $Z/28Z$.

Сравнить количество этих элементов с $\varphi(11)$ и $\varphi(28)$ соответственно.

Является ли эта группа относительно умножения циклической?

Вариант 5

1. Множество целых чисел с операцией умножения.

2. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 5 & 6 & 7 & 8 & 9 & 2 & 1 \end{pmatrix}$.

3. $B = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$.

4. Выписать все элементы мультипликативной группы кольца:

а) $Z/18Z$;

б) $Z/31Z$.

Сравнить количество этих элементов с $\varphi(18)$ и $\varphi(31)$ соответственно.

Является ли эта группа относительно умножения циклической?

Вариант 6

1. Множество вещественных чисел с операцией деления.

2. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 6 & 5 & 1 & 7 & 2 & 3 & 4 & 8 \end{pmatrix}$.

3. $B = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$.

4. Выписать все элементы мультипликативной группы кольца:

а) $Z/29Z$;

б) $Z/16Z$.

Сравнить количество этих элементов с $\varphi(29)$ и $\varphi(16)$ соответственно.

Является ли эта группа относительно умножения циклической?

Вариант 7

1. Множество комплексных чисел с операцией $z_1 \otimes z_2 = \sqrt{z_1 z_2}$.

2. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 1 & 6 & 3 & 7 & 4 & 5 & 2 \end{pmatrix}$.

3. $B = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$.

4. Выписать все элементы мультипликативной группы кольца:

а) $Z/17Z$;

б) $Z/26Z$.

Сравнить количество этих элементов с $\varphi(17)$ и $\varphi(26)$ соответственно.

Является ли эта группа относительно умножения циклической?

Вариант 8

1. Множество комплексных чисел с операцией деления.

2. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 8 & 7 & 5 & 9 & 3 & 6 & 1 & 2 \end{pmatrix}$.

3. $B = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$.

4. Выписать все элементы мультипликативной группы кольца:

а) $Z/23Z$;

б) $Z/24Z$.

Сравнить количество этих элементов с $\varphi(23)$ и $\varphi(24)$ соответственно.

Является ли эта группа относительно умножения циклической?

Вариант 9

1. Множество целых чисел с операцией вычитания?

2. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 6 & 5 & 1 & 7 & 2 & 8 & 4 & 3 \end{pmatrix}$.

3. $B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$.

4. Выписать все элементы мультипликативной группы кольца:

а) $Z/23Z$;

б) $Z/21Z$.

Сравнить количество этих элементов с $\varphi(23)$ и $\varphi(21)$ соответственно. Является ли эта группа относительно умножения циклической?

Вариант 10

1. Множество всех положительных вещественных чисел с операцией деления.

2. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 5 & 6 & 1 & 7 & 2 & 8 & 4 & 3 \end{pmatrix}$.

3. $B = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$.

4. Выписать все элементы мультипликативной группы кольца:

а) $Z/31Z$;

б) $Z/20Z$.

Сравнить количество этих элементов с $\varphi(31)$ и $\varphi(20)$ соответственно.

Является ли эта группа относительно умножения циклической?

Вариант 11

1. Множество целых чисел с операцией $m * n = mn + m$.

2. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 6 & 5 & 7 & 1 & 2 & 8 & 4 & 3 \end{pmatrix}$.

3. $B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}$.

4. Выписать все элементы мультипликативной группы кольца:

а) $Z/14Z$;

б) $Z/37Z$.

Сравнить количество этих элементов с $\varphi(14)$ и $\varphi(37)$ соответственно.

Является ли эта группа относительно умножения циклической?

Вариант 12

1. Множество целых чисел с операцией $m * n = m + 2n$.

2. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 6 & 5 & 1 & 7 & 4 & 8 & 2 & 3 \end{pmatrix}$.

3. $B = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$.

4. Выписать все элементы мультипликативной группы кольца

а) $Z/17Z$;

б) $Z/25Z$.

Сравнить количество этих элементов с $\varphi(17)$ и $\varphi(25)$ соответственно.

Является ли эта группа относительно умножения циклической?

Вариант 13

1. Все комплексные числа верхней полуплоскости относительно умножения.

2. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 6 & 2 & 1 & 7 & 5 & 8 & 4 & 3 \end{pmatrix}$.

3. $B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$.

4. Выписать все элементы мультипликативной группы кольца:

а) $Z/17Z$;

б) $Z/27Z$.

Сравнить количество этих элементов с $\varphi(17)$ и $\varphi(27)$ соответственно.

Является ли эта группа относительно умножения циклической?

Вариант 14

1. Комплексные числа правой полуплоскости относительно умножения.

2. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 6 & 5 & 1 & 7 & 2 & 4 & 8 & 3 \end{pmatrix}$.

3. $B = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$.

4. Выписать все элементы мультипликативной группы кольца:

а) $Z/13Z$;

б) $Z/22Z$.

Сравнить количество этих элементов с $\varphi(13)$ и $\varphi(22)$ соответственно.

Является ли эта группа относительно умножения циклической?

Вариант 15

1. Комплексные числа нижней полуплоскости относительно умножения.

2. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 6 & 5 & 1 & 7 & 2 & 4 & 8 & 3 \end{pmatrix}$.

3. $B = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$.

4. Выписать все элементы мультипликативной группы кольца:

а) $Z/15Z$;

б) $Z/29Z$.

Сравнить количество этих элементов с $\varphi(15)$ и $\varphi(29)$ соответственно.

Является ли эта группа относительно умножения циклической?

Лабораторная работа № 5

КРИПТОСИСТЕМА *RSA*. КИТАЙСКАЯ ТЕОРЕМА ОБ ОСТАТКАХ

Цель работы: изучение шифрования с помощью криптосистемы *RSA* с применением китайской теоремы об остатках.

Необходимые теоретические сведения

Криптосистема RSA

Наиболее популярной современной системой с открытым ключом является *RSA*-криптосистема (Rivest R., Shamir A., Adleman L.). Берутся 2 больших простых числа p и q. Вычисляется их произведение $n = p \cdot q$. Тогда $\varphi(n) = (p-1)(q-1)$. Выбираем натуральное число e, такое, что $0 < e < n$ и НОД $(e, \varphi(n)) = 1$.

Пара (e, n) и будет открытым ключом. Шифруемая информация переводится в цифровую форму. Например, в первоисточнике буквы латинского алфавита заменялись двузначными числами: «*a*» = 01, «*b*» = 02, …, пробел = 00. Получается некоторое число *c*. Предполагается, что, $0 < c < n$ и НОД$(c, n) = 1$. Сообщение передается числом $ш = c^e \pmod n$.

Адресат получает сообщение $(ш, e, n)$. Он, как и все, знает n и e. Он также должен знать секретный ключ – такое натуральное $d < n$, что $e \cdot d \equiv 1 (\mathrm{mod}(\varphi(n)))$. Значит, $e \cdot d = \varphi(n) \cdot k + 1$ для некоторого целого *k*. Тогда по теореме Эйлера $ш^d = c^{ed} = c \cdot (c^{\varphi(n)})^k \equiv c \cdot 1 = c \pmod n$. Итак, для нахождения c достаточно найти остаток от деления $ш^d$ на n.

Взломать криптотекст *RSA* можно, только если найти $d -$ решение сравнения $ed \equiv 1 (\mathrm{mod}\, \varphi(n))$. Для этого надо знать $\varphi(n)$. Из свойств $\varphi(n)$ следует, что единственно надежный путь для этого – разложить n на множители – трудоемкая задача, составляющая основу криптографической стойкости криптосистемы *RSA*.

Пример 5.1. Зашифруем системой *RSA* слово «сад». Его цифровым аналогом в соответствии с выше принятым правилом будет число $c = 190105$. Возьмем два простых числа $p = 47$ и $q = 71$. Тогда открытый ключ $n = p \cdot q = 3337$. Находим $\varphi(n) = 46 \cdot 70 = 3220$. Выберем $e = 79$, такое, что НОД $(79, 3220) = 1$. У нас $c > n$. Поэтому для шифрования сообщения c разделим его на блоки c_1, c_2 так, чтобы $0 < c_i < 3337$, $i = 1, 2$. Возьмем $c_1 = 190$; $c_2 = 105$. Запишем $e = 79$ в двоичной системе счисления: $79_{10} = 1001111_2 = 2^6 + 2^3 + 2^2 + 2 + 1 = 64 + 8 + 4 + 2$.

Первый блок шифруется так:

$190^2 = 36100 \equiv 2730 \pmod{3337}$;

$190^4 \equiv 2730^2 = 7452900 \equiv 1379 \pmod{3337}$;

$190^8 \equiv 1379^2 = 1901641 \equiv 2888 \pmod{3337}$;

$190^{16} \equiv 2888^2 = 8340544 \equiv 1381 \pmod{3337}$;

$190^{32} \equiv 1381^2 = 1907161 \equiv 1734 \pmod{3337}$;

$190^{64} \equiv 1734^2 = 3006756 \equiv 119 \pmod{3337}$;

$190^{79} \equiv 119 \cdot 2888 \cdot 1379 \cdot 2730 \cdot 190 \equiv 742 \pmod{3337}$.

Второй блок: $105 = 105 \pmod{3337}$; $105^2 \equiv 1014 \pmod{3337}$;

$105^4 = 1014^2 \equiv 400 \pmod{3337}$; $105^8 \equiv 400^2 \equiv 3161 \pmod{3337}$;

$105^{16} \equiv 3161^2 \equiv 943 \pmod{3337}$; $105^{32} \equiv 943^2 \equiv 1607 \pmod{3337}$;

$105^{64} \equiv 1607^2 \equiv 2948 \pmod{3337}$.

Тогда $105^{79} \equiv 2948 \cdot 3161 \cdot 400 \cdot 1014 \cdot 105 \equiv 193 \pmod{3337}$.

Передаваемые сообщения: (742, 79, 3337) и (193, 79, 3337). Конечно, адресат должен знать о разбиении сообщения на блоки. Отметим также, что для большей криптостойкости лучше было бы сообщение не разбивать на блоки, а выбрать $n > c$.

Китайская теорема об остатках – *CRT*

Такое название носит следующая теорема.

Теорема 5.1. Пусть $m = m_1 \cdot m_2 \cdot ... \cdot m_n$ – разложение натурального числа m в произведение попарно взаимно простых множителей. Пусть $b_1, b_2, ..., b_n$ – произвольные фиксированные целые числа. Тогда система сравнений $\begin{cases} x \equiv b_1 (\mathrm{mod}\, m_1), \\ ..... \\ x \equiv b_n (\mathrm{mod}\, m_n) \end{cases}$ всегда имеет решения и все они сравнимы друг с другом по модулю m.

Экзотичность названия теоремы объясняется тем, что исторически впервые она рассматривалась в китайском «Учебнике математики мастера Сана», написанном между 287 и 473 годами нашей эры.

Определение 5.1. Каждое целое число x в условиях теоремы 5.1, имеет n остатков b_i от деления на каждый из делителей m_i числа m. Набор $(b_1, b_2, ..., b_n)$ называется *CRT-представлением* числа x.

CRT-теорема утверждает, что существует бесконечно много целых чисел $\tilde{x}$ с таким же набором $(b_1, b_2, ..., b_n)$ остатков от деления на числа m_i, однако все они сравнимы друг с другом по модулю m, то есть отстоят друг от друга на число, кратное m: $\tilde{x} = x + mq$ для подходящего целого q. В частности, отсюда следует, что в кольце Z/mZ число x с данным набором $(b_1, b_2, ..., b_n)$ единственно. Таким образом, мы обосновали первое следствие.

Следствие 5.1. *CRT*-теорема устанавливает взаимно однозначное соответствие между целыми числами на отрезке от нуля до $m-1$ включительно и всеми возможными наборами чисел $(b_1, b_2, ..., b_n)$ для целых b_i на отрезке от нуля до $m_i - 1$ включительно: $x \leftrightarrow (b_1, b_2, ..., b_n)$.

Установленное следствием 1 соответствие сохраняет и арифметические операции над числами в силу свойств сравнений.

Следствие 5.2. *Если* $x \leftrightarrow (b_1, b_2, ..., b_n)$, $y \leftrightarrow (c_1, c_2, ..., c_n)$, то

$(x \pm y) \bmod m \leftrightarrow ((b_1 \pm c_1) \bmod m_1, (b_2 \pm c_2) \bmod m_2, ..., (b_n \pm c_n) \bmod m_n)$;

$(x \cdot y) \bmod m \leftrightarrow ((b_1 \cdot c_1) \bmod m_1, (b_2 \cdot c_2) \bmod m_2, ..., (b_n \cdot c_n) \bmod m_n)$;

$(x \cdot y^{-1}) \bmod m \leftrightarrow ((b_1 \cdot c_1^{-1}) \bmod m_1, (b_2 \cdot c_2^{-1}) \bmod m_2, ..., (b_n \cdot c^{-1}{}_n) \bmod m_n)$

для $y \in U(m)$.

Из свойств взаимно простых чисел и следствия 1 вытекает следующее.

Следствие 5.3. В условиях следствия 1 класс $\bar{x}$ обратим в кольце Z/mZ тогда и только тогда, когда в соответствующем числу x наборе $(b_1, b_2, ..., b_n)$ каждая координата b_i порождает обратимый класс в Z/m_iZ.

Теорема 5.2. Если $m = m_1 \cdot m_2 \cdot ... \cdot m_n$ – разложение натурального числа m в произведение попарно взаимно простых множителей, то $U(m) \cong U(m_1) \times U(m_2) \times ... \times U(m_n)$ – мультипликативная группа $U(m)$ обратимых элементов кольца Z/mZ – изоморфна прямому произведению мультипликативных групп $U(m_i)$ колец Z/m_iZ, $1 \le i \le n$.

Напомним, что прямое произведение абелевых групп $G_1, G_2, ..., G_n$ есть группа G, состоящая из всевозможных элементов вида $g = (g_1, g_2, ..., g_n)$. В случае сомножителей конечного порядка эта абелева группа имеет порядок $|G| = |G_1| \cdot |G_2| \cdot ... \cdot |G_n|$, а каждый элемент группы G имеет порядок, равный наименьшему общему кратному порядков сомножителей g_i.

Согласно теореме Эйлера $g^{\varphi(m)} = 1$ для каждого $g \in U(m)$. Из теоремы 5.2 вытекает важное для приложений следствие.

Следствие 5.4. Для наименьшего общего кратного τ чисел $\varphi(m_1), \varphi(m_2), ..., \varphi(m_n)$ и для каждого элемента $g \in U(m)$ в условиях теоремы 5.2 имеет место равенство: $g^{\tau} = 1$.

Согласно следствию 1 арифметические действия с числами по модулю m можно заменить на такие же, но с *CRT*-представлениями этих чисел. На первый взгляд, такой переход кажется громоздким, но для операций с числами большой

разрядности, явно выходящей за общепринятый в применяемых компьютерах диапазон, такой переход оправдан и приносит существенный выигрыш в количестве операций. Уже при разложении m в произведение двух взаимно простых сомножителей (как в криптосистеме *RSA*) умножение *CRT*-представлений приводит примерно к двукратному выигрышу в количестве операций, то есть к двукратному выигрышу во времени.

Еще больший выигрыш – трехкратный, а то и четырехкратный – получается при возведении чисел в степень.

Пример 5.2. Найдем $23^{17} \pmod{35}$.

Решение. Традиционный путь мы знаем. $23^2 = 529 = 35 \cdot 15 + 4 \equiv 4 \pmod{35}$;

$23^4 \equiv 16 \pmod{35}$; $23^8 \equiv 256 \pmod{35} = (35 \cdot 7 + 11) \pmod{35} \equiv 11 \pmod{35}$;

$23^{16} \equiv 121 \pmod{35} \equiv 16 \pmod{35}$.

Тогда $23^{17} = 23^{16} \cdot 23 \equiv 16 \cdot 23 \pmod{35} \equiv 18 \pmod{35}$.

Попробуем эту же задачу решить через *CRT*-представление. Поскольку $35 = 5 \cdot 7$ и $23 \equiv 3 \pmod{5}$; $23 \equiv 2 \pmod{7}$, то *CRT*-представлением числа 23 является пара (3, 2). Здесь $\varphi(5) = 4$, $\varphi(7) = 6$. Поэтому наименьшее общее кратное $\tau = 12$. Следовательно, $3^{17} \equiv 3^5 \pmod{5} \equiv 3 \pmod{5}$; $2^{17} \equiv 2^5 \pmod{7} \equiv 4 \pmod{7}$. Таким образом, $23^{17} \pmod{35}$ имеет *CRT*-представление – пару (3, 4), которая, очевидно, представляет число $18 \pmod{35}$.

Уже на этом примере ощущаем легкость вычислений с *CRT*-представлением по сравнению с тяжеловесностью прямого пути.

Осталось обсудить вопрос о восстановлении элемента $x \in Z/mZ$ по известному его *CRT*-представлению (в примере 5.2 все числа малые, поэтому x легко угадывался, это несколько затушевывает проблему, поскольку в общем случае значение x далеко не очевидно).

Задачу о восстановлении элемента $x \in Z/mZ$ по известному его *CRT*-представлению можно решить рекуррентно из следующей рекуррентной системы уравнений-сравнений:

$$\begin{cases} y_1 = b_1 \bmod m_1; \\ y_2 = N_2\left(\left(C_2(b_2 - y_1)\right)\bmod m_2\right) + y_1; \\ y_3 = N_3\left(\left(C_3(b_3 - y_2)\right)\bmod m_3\right) + y_2; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ y_n = N_n\left(\left(C_n(b_n - y_{n-1})\right)\bmod m_n\right) + y_{n-1}. \end{cases} \quad (5.1)$$

Здесь $N_i = m_1 \cdot m_2 \cdot \ldots \cdot m_{i-1}$; коэффициенты C_i находятся из условия: $C_i N_i \equiv 1 (\bmod m_i)$. Число y_n и будет единственным решением системы сравнений из теоремы 5.2, принадлежащим отрезку $[0;\ n-1]$.

Проверим корректность выписанной системы уравнений-сравнений для наиболее популярного случая $n = 2,$ который реализован в криптосистеме *RSA*. Будем при этом пользоваться соответствующими обозначениями. Итак, $m = m_1 \cdot m_2 = p \cdot q -$ произведение двух простых чисел. Пусть a и $b -$ целые числа, такие, что $0 \le a < p$ и $0 \le b < q.$ Согласно *CRT* система сравнений $\begin{cases} x \equiv a \bmod p; \\ x \equiv b \bmod q \end{cases}$ имеет единственное решение на множестве целых чисел от нуля до $m-1$ включительно. В этом случае система (5.1) состоит из первых двух уравнений. При этом $N_2 = m_1 = p;$ $C_2 -$ обратный к $N_2 = p$ в кольце Z/qZ $C_2 = p^{-1} \bmod q.$ Подставляя в (5.1) при $n = 2$ эти данные и значения $y_1 = a,$ $b_2 = b,$ получаем, что это решение находится из следующей формулы:

$$x = \left(\left((b-a)(p^{-1} \bmod q)\right)\bmod q\right)p + a. \quad (5.2)$$

Меняя в этой формуле p и q местами, получим формулу

$$x = \left(\left((a-b)(q^{-1} \bmod p)\right)\bmod p\right)q + b, \quad (5.3)$$

которая носит название *формулы Гарнера* (Garner's formula).

Пример 5.3. $19(\bmod 143) = 19(\bmod 11 \cdot 13)$ имеет *CRT*-представлением пару (8, 6). Следовательно, 19 должно быть одним из решений системы сравнений

$\begin{cases} x \equiv 8 \bmod 11 \\ x \equiv 6 \bmod 13 \end{cases}$. Согласно приведенной теории, это число можно восстановить по формулам (5.2) или (5.3). Попробуем убедиться в этом.

Для решения поставленной задачи надо предварительно вычислить $13^{-1} \bmod 11$ и $11^{-1} \bmod 13$. Ясно, что $13 \bmod 11 = 2;\ \ 2 \cdot 6 = 12 \equiv 1 \bmod 11,$ поэтому $13^{-1} \bmod 11 = 6.$

Величину $11^{-1} \bmod 13$ найдем расширенным алгоритмом Евклида для НОД $(11, 13) = 1:\ 13 = 11 \cdot 1 + 2;\ 11 = 2 \cdot 5 + 1.$

Следовательно, $1 = 11 \cdot 1 + 2 \cdot (-5) = 11 \cdot 1 + (13 \cdot 1 + 11 \cdot (-1))(-5) = 13 \cdot (-5) + 11 \cdot 6.$ Отсюда получаем: $11^{-1} \bmod 13 = 6.$ Согласно формуле (5.2)

$$x = ((6-8)6 \bmod 13)11 + 8 = (-12(\bmod 13))11 + 8 = 11 + 8 = 19.$$

Согласно формуле (5.3) $x = ((8-6)6 \bmod 11)13 + 6 = 13 + 6 = 19.$ Формулы работают правильно.

Задания для аудиторной работы

Задание 1. Зашифровать в системе *RSA* сообщение $c = 51$.

Решение. Выбираем число n, $0 < c < n$, являющееся произведением простых чисел p и q и взаимно простого с c. Например, $n = 55 = 5 \cdot 11$ $p = 5,\ \ q = 11,$ и НОД$(51, 55) = 1$. Находим функцию $\varphi(n) = (p-1)(q-1)$. $\varphi(55) = 40$. Далее выбираем e, такое, что НОД$(e, \varphi(n)) = 1$. Например, $e = 3$. Возводим c в степень e по модулю $n = 55.$ Это и будет передаваемое сообщение: $51^3 = 132651 \equiv 46(\bmod 55).$

Пара (3, 55) – открытый ключ. Передаваемое сообщение (46, 3, 55).

Задание 2. Расшифровать в системе *RSA* (46, 3, 55).

Решение.

1) Раскладываем n на простые множители: $55 = 5 \cdot 11.\ \ p = 5,\ \ q = 11.$

2) Находим значение функции Эйлера $\varphi(n)$. В данном случае $\varphi(55) = 4 \cdot 10 = 40$.

3) Находим секретный ключ d из соотношения Безу: $3u + 40v = 1$, получаемого обратной прогонкой алгоритма Евклида для нахождения $\text{НОД}(3, 40) = 1$. В данном случае алгоритм Евклида предельно краток: $40 = 13 \cdot 3 + 1$. Следовательно, $1 = 1 \cdot 40 + (-13) \cdot 3$. Поэтому в кольце $Z/40Z$ $\overline{3}^{-1} = \overline{-13} = \overline{40 - 13} = \overline{27}$. Таким образом, $d = 27$.

4) Находим $ш^d \equiv c (\text{mod}\, n)$, то есть $46^{27} (\text{mod}\, 55) = c$. Для этого переводим d в двоичную систему счисления:

$$d = 27_{10} = 11011_2 = 2^4 + 2^3 + 2^1 + 2^0 = 16 + 8 + 2 + 1.$$

$$46^2 \equiv 26 (\text{mod}\, 55); \quad 46^4 \equiv 26^2 \equiv 16 (\text{mod}\, 55); \quad 46^8 \equiv 16^2 \equiv 36 (\text{mod}\, 55);$$

$$46^{16} \equiv 36^2 \equiv 31 (\text{mod}\, 55); \quad 46^{27} \equiv 31 \cdot 36 \cdot 26 \cdot 46 = 1334736 \equiv 51 (\text{mod}\, 55).$$

Ответ: $c = 51$.

Задание 3. Зашифровать в системе *RSA* сообщение $c = 156$.

Решение. Выбираем $n = 209 = 11 \cdot 19$, $p = 11$, $q = 19$, такое, что $156 < 209$ и НОД (156, 209) = 1. Здесь $\varphi(209) = \varphi(11) \cdot \varphi(19) = 10 \cdot 18 = 180$.

Выбираем $e = 7$ такое, что $\text{НОД}(7,\ 180) = 1$. Тогда шифровка $ш \equiv c^e = 156^7 (\text{mod}\, 209)$. $e = 7_{10} = 111_2 = 2^2 + 2 + 1 = 4 + 2 + 1$;

$156^7 \equiv 156^4 \cdot 156^2 \cdot 156 (\text{mod}\, 209)$;

$156^2 = 24336 \equiv 92 (\text{mod}\, 209)$; $156^4 \equiv 92^2 = 8464 \equiv 104 (\text{mod}\, 209)$;

$156^7 \equiv 156 \cdot 92 \cdot 104 = 1492608 \equiv 139 (\text{mod}\, 209)$.

Пара (7, 209) – открытый ключ. Передаваемое сообщение (139, 7, 209).

Задание 4. Расшифровать сообщение (139, 7, 209).

Решение.

1) Раскладываем $n = 209$ на простые множители $209 = p \cdot q = 11 \cdot 19$.

2) Находим $\varphi(209) = (p-1)(q-1) = 10 \cdot 18 = 180$.

3) Находим секретный ключ d с помощью алгоритма Евклида.

$$180 = 25 \cdot 7 + 5;$$

$$7 = 1 \cdot 5 + 2;$$

$$5 = 2 \cdot 2 + 1.$$

Поэтому:

$1 = 5 + (-2) \cdot 2 = 5 + (-2) \cdot (7 - 1 \cdot 5) = 5 + (-2) \cdot 7 + 2 \cdot 5 = (-2) \cdot 7 + 3 \cdot 5 = (-2) \cdot 7 + 3(180 - 25 \cdot 7) =$
$= 3 \cdot 180 + (-77) \cdot 7.$

Следовательно, $\overline{e^{-1}} = \overline{-77} = \overline{180 - 77} = \overline{103}.$ Значит, $d = 103$.

4) Находим $w^d \equiv c \pmod{n}$, то есть $139^{103} \pmod{209}$.

$103_{10} = 1110011_2 = 2^6 + 2^5 + 2^2 + 2 + 1 = 64 + 32 + 4 + 3.$

$139^2 \equiv 93 \pmod{209}$; $139^4 \equiv 93^2 \equiv 80 \pmod{209}$; $139^8 \equiv 80^2 \equiv 130 \pmod{209}$;

$139^{16} \equiv 130^2 \equiv 180 \pmod{209}$; $139^{32} \equiv 180^2 \equiv 5 \pmod{209}$;

$139^{64} \equiv 5^2 = 25 \pmod{209}$; $139^{103} \equiv 25 \cdot 5 \cdot 80 \cdot 93 \cdot 139 = 129270000 \equiv 156 \pmod{209}$.

Ответ: присланное сообщение $c = 156$.

Задание 5. Зашифровать сообщение «Ау» по схеме *RSA*, используя китайскую теорему об остатках.

Решение. Как и в первом задании перейдем к числовому эквиваленту сообщения $ay \leftrightarrow 121$. Выберем простые числа p и q так, чтобы их произведение $n = pq$ было больше $c = 121$ и взаимно просто с ним. Возьмем $p = 7$ и $q = 19$. Тогда $n = pq = 133$ удовлетворяет требуемым условиям. Положим $e = 41$. Следует вычислить $w = c^e \bmod(n) = 121^{41} (\bmod 133)$. Найдем CRT-представление $c = 121 \leftrightarrow (2, 7)$. $\varphi(n) = 6 \cdot 18 = 108$. $\text{НОК}(6, 18) = 18$. Следовательно, для всякого $a \in Z/133Z$ $a^{18} = 1$. Поэтому $121^{41} = 121^5 (\bmod 133)$. Найдем пятые степени компонент CRT-представления числа c. $2^5 \equiv 4 (\bmod 7)$. $7^5 = 49 \cdot 49 \cdot 7 \equiv 11 \cdot 11 \cdot 7 (\bmod 19) \equiv 11 (\bmod 19)$. Таким образом, $w \leftrightarrow (4, 11)$.

Очевидно, такое CRT-представление имеет число 11. Значит, $ш = 11$. Итак, по схеме *RSA* построено сообщение $(n, e, ш) = (133, 41, 11)$.

Задание 6. Расшифровать сообщение $(n, e, ш) = (133, 41, 11)$, используя китайскую теорему об остатках.

Решение. Основа стойкости криптосистемы *RSA* – сложность разложения $n = 133$ на простые множители здесь преодолевается элементарно: $133 = 19 \cdot 7$. Тогда $\varphi(133) = 6 \cdot 18 = 108 = 2^2 \cdot 3^3$, а $\text{НОК}(\varphi(7), \varphi(19)) = 18$. Необходимо найти $d = e^{-1} = 41^{-1}$ в кольце $Z/108Z$. $\varphi(108) = \varphi(2^2) \cdot \varphi(3^3) = 2 \cdot 18 = 36$, а $\text{НОК}(\varphi(2^2), \varphi(3^3)) = 18$. Следовательно, для всякого $a \in Z/108Z$ $a^{18} = 1$, в частности, $41^{18} = 1$. Поэтому в кольце $Z/108Z$ $41^{-1} = 41^{17}$. Вычислим эту величину. $41^2 = 1681 \equiv 61 (\text{mod} 108)$; $41^4 \equiv 61^2 = 3721 \equiv 49 (\text{mod} 108)$; $41^8 \equiv 25 (\text{mod} 108)$; $41^{17} \equiv 85 \cdot 41 \equiv 29 (\text{mod} 108)$. Следовательно, $41^{17} \equiv 85 \cdot 41 \equiv 29 (\text{mod} 108)$. Итак, в кольце $Z/108Z$ $41^{-1} = 29$.

Расшифровка сообщения заключается в вычислении $c = ш^d (\text{mod}\, n) = 11^{29} (\text{mod} 133)$. Учитывая отмеченный в решении предыдущего задания факт того, что для всякого $a \in Z/133Z$ $a^{18} = 1$, видим, что $11^{29} = 11^{18+11} \equiv 11^{11} (\text{mod} 133)$. Перейдем к *CRT*-представлению: $11^{11} \leftrightarrow (4^{11}, 11^{11})$. В силу малой теоремы Ферма $4^6 \equiv 1 (\text{mod}\, 7)$. Поэтому $4^{11} \equiv 4^5 (\text{mod}\, 7) = 16 \cdot 16 \cdot 4 (\text{mod}\, 7) \equiv 2 (\text{mod}\, 7)$. Теперь вычислим $11^{11} (\text{mod} 19)$. $11^2 \equiv 7 (\text{mod} 19)$; $11^3 \equiv 11 \cdot 7 = 19 \cdot 4 + 1 \equiv 1 (\text{mod} 19)$.

Поэтому $11^{11} \equiv 11^{3+3+3+2} \equiv 11^2 (\text{mod} 19) \equiv 7 (\text{mod} 19)$. Таким образом, $c \leftrightarrow (2, 7)$. Восстановим c по его *CRT*-представлению с помощью формулы (5.3) $c = (((a - b)(q^{-1} \bmod p)) \bmod p) q + b$. Здесь $q^{-1} (\text{mod}\, p) = 19^{-1} (\text{mod}\, 7) = 5^{-1} (\text{mod}\, 7) = 3$. Тогда $c = (((2 - 7)3) \bmod 7) 19 + 7 = 6 \cdot 19 + 7 = 121$. Следовательно, передано сообщение «Ау». Задание полностью решено.

Индивидуальные задания

1. Расшифровать три сообщения (криптосистема *RSA* без применения *CRT*).
2. Расшифровать с помошью *CRT*.

Вариант 1

1. а) $n = 21,\ e = 7,\ ш = 2$; б) $n = 2021,\ e = 11,\ ш = 1791$;

   в) $n = 250483,\ e = 13,\ ш = 242215$.

2. p = 2038074743;

   q = 2038074751;

   e = 1299709.

   Шифр: 24280100060807223l1.

Вариант 2

1. а) $n = 15,\ e = 3,\ ш = 13$; б) $n = 2021,\ e = 5,\ ш = 1265$;

   в) $n = 1269083,\ e = 13,\ ш = 1101727$.

2. p = 2038074761;

   q = 2038074769;

   e = 1299709.

   Шифр: 5914054053157757 98.

Вариант 3

1. а) $n = 21,\ e = 7,\ ш = 13$; б) $n = 589,\ e = 7,\ ш = 109$;

   в) $n = 3338287,\ e = 19683,\ ш = 2092819$.

2. p = 2038074793;

   q = 2038074803;

   e = 1299709.

   Шифр: 33245715266345021l2.

Вариант 4

1. а) $n = 35,\ e = 11,\ ш = 31;$ б) $n = 1147,\ e = 7,\ ш = 1064;$

в) $n = 1897613,\ e = 161051,\ ш = 939402.$

2. p = 2038074743;

   q = 2038074751;

   e = 1299709.

   Шифр: 946136620149391608.

Вариант 5

1. а) $n = 77,\ e = 13,\ ш = 31;$ б) $n = 1147,\ e = 13,\ ш = 576;$

в) $n = 1457297,\ e = 1331,\ ш = 1155557.$

2. p = 2038074761;

   q = 2038074769;

   e = 1299709.

   Шифр: 154793207506590481.

Вариант 6

1. а) $n = 35,\ e = 7,\ ш = 2;$ б) $n = 2021,\ e = 5,\ ш = 997;$

в) $n = 5994581,\ e = 29575,\ ш = 1452748.$

2. p = 2038074793;

   q = 2038074803;

   e = 1299709.

   Шифр: 48212856809741423.

Вариант 7

1. а) $n = 35,\ e = 7,\ ш = 7;$ б) $n = 2021,\ e = 773,\ ш = 2017;$

в) $n = 4116037,\ e = 451737,\ ш = 833207.$

2. p = 2038074743;

q = 2038074751;

e = 1299709.

Шифр: 30164155432485365 77

Вариант 8

1. а) $n = 35,\ e = 7,\ ш = 13;$ б) $n = 2021,\ e = 527,\ ш = 2017;$

в) $n = 16440383,\ e = 4225,\ ш = 6188609.$

2. p = 2038074761;

q = 2038074769;

e = 1299709.

Шифр: 37239602198955744 53.

Вариант 9

1. а) $n = 35,\ e = 7,\ ш = 8;$ б) $n = 2021,\ e = 773,\ ш = 1237;$

в) $n = 15678841,\ e = 1521,\ ш = 3924343$.

2. p = 2038074793;

q = 2038074803;

e = 1299709.

Шифр: 7212010765654264 06.

Вариант 10

1. а) $n = 35,\ e = 3,\ ш = 8;$ б) $n = 2021,\ e = 527,\ ш = 1237;$

в) $n = 120287593,\ e = 29403,\ ш = 115658693.$

2. p = 2038074743;

q = 2038074751;

e = 1299709.

Шифр: 30017057801047480 30.

Вариант 11

1. а) $n = 15,\ e = 11,\ ш = 7$; б) $n = 589,\ e = 77,\ ш = 97$;

в) $n = 91322059,\ e = 105625,\ ш = 24893033.$

2. p = 2038074761;

q = 2038074769;

e = 1299709.

Шифр: 1881414812857795554.

Вариант 12

1. а) $n = 33,\ e = 9,\ ш = 20$; б) $n = 1147,\ e = 164,\ ш = 691$;

в) $n = 4144226923,\ e = 20449,\ ш = 708173492$.

2. p = 380747934;

q = 2038074803;

e = 1299709;

Шифр: 39830648623199853 75.

Вариант 13

1. а) $n = 21,\ e = 7,\ ш = 2$; б) $n = 2021,\ e = 11,\ ш = 1791$;

в) $n = 250483,\ e = 13,\ ш = 242215$.

2. p = 2038074743;

q = 2038074751;

e = 1299709.

Шифр: 16448614810495190 42

Вариант 14

1. а) $n = 15,\ e = 3,\ ш = 13$; б) $n = 2021,\ e = 5,\ ш = 1265$;

в) $n = 1269083,\ e = 13,\ ш = 1101727$.

2. p = 2038074761;

q = 2038074769;

e = 1299709;

Шифр: 34437191752117366608.

Вариант 15

1. а) $n = 21,\ e = 7,\ ш = 13$; б) $n = 589,\ e = 7,\ ш = 109$;

   в) $n = 3338287,\ e = 19683,\ ш = 2092819$.

2. p = 2038074793;

   q = 2038074803;

   e = 1299709.

   Шифр: 31959869282855325l6.

Лабораторная работа № 6
КВАДРАТИЧНЫЕ ВЫЧЕТЫ. КРИПТОСИСТЕМА РАБИНА

Цель работы: изучение квадратичных вычетов и шифрования с помощью криптосистемы Рабина.

Необходимые теоретические сведения

Квадратичные вычеты

Определение 6.1. Пусть n – целое число и $n>1$. Число a из Z/nZ называется *квадратичным вычетом по модулю* n $(quadratic\ residue\ modulo\ n)$, если в Z/nZ существует число x, удовлетворяющее условию $x^2 \equiv a(\mathrm{mod}\, n)$, в противном случае число a называется *квадратичным невычетом по модулю* n $(quadratic\ nonresidue\ modulo\ n)$.

Множество квадратичных вычетов по модулю n обозначается как QR_n, а невычетов – как QNR_n.

Пример 6.1. Вычислим QR_{11} – множество всех квадратичных вычетов по модулю 11.

$$QR_{11} = \{1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2\}(\mathrm{mod}11) = \{1, 3, 4, 5, 9\}.$$

Но на самом деле достаточно возвести в квадрат по модулю 11 лишь половину элементов $Z/11Z^*$: $QR_{11} = \{1^2, 2^2, 3^2, 4^2, 5^2\}(\mathrm{mod}11)$. Этот факт обобщается в следующей теореме.

Теорема 6.1. Пусть p – простое число. Тогда справедливы следующие утверждения:

1. $QR_p = \left\{ x^2 (\mathrm{mod}\ p) \,\middle|\, 0 < x \le \frac{p-1}{2} \right\}$.

2. Существует ровно $\frac{p-1}{2}$ квадратичных вычетов по модулю p, т. е. Z/pZ^* разбивается на два подмножества QR_p и QNR_p, состоящих из одинакового количества элементов.

Следствие 6.1. Пусть p – простое число. Тогда любое число $a \in QR_p$ имеет ровно два квадратных корня по модулю p. Обозначим один из них буквой x, тогда второй корень равен

$$-x = p - x.$$

Теорема 6.2 (Критерий Эйлера). Пусть p – простое число. Для любого числа $x \in Z/pZ^*$ условие $x \in QR_p$ выполняется тогда и только тогда, когда

$$x^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p).$$

Вычисление квадратичных корней по простому модулю

Случай $p \equiv 3,7 (\mathrm{mod}\, 8)$.

Для $a \in QR_p$ его квадратным корнем по модулю p будет

$$x_p = a^{\frac{p+1}{4}} (\mathrm{mod}\, p).$$

Теорема 6.3. Пусть n – составное число. $n = p_1^{l_1} \cdot p_2^{l_2} \cdot \ldots \cdot p_k^{l_k}$. Число $x \in QR_n$ тогда и только тогда, когда $x (\mathrm{mod}\, p_i) \in QR_{p_i}$, где $p_i (i = 1, 2, \ldots, k)$ – простые числа.

Вычисление квадратных корней по составному модулю

Если $n = p \cdot q$, где p и q – простые числа, отношение

$$x^2 \equiv y (\mathrm{mod}\, n)$$

выполняется тогда и только тогда, когда оно справедливо как по модулю p, так и по модулю q.

Число $y \in QR_n$ имеет в Z/nZ^* ровно четыре квадратных корня, которые вычисляются так:

$$x_1 = \begin{cases} x_p \pmod p \\ x_q \pmod q \end{cases},$$

$$x_2 = \begin{cases} x_p \pmod p \\ (q - x_q) \pmod q \end{cases},$$

$$x_3 = \begin{cases} (p - x_p) \pmod p \\ x_q \pmod q \end{cases},$$

$$x_4 = \begin{cases} (p - x_p) \pmod p \\ (q - x_q) \pmod q \end{cases}.$$

Теорема 6.4. Пусть $n = p \cdot q$, где p и q – разные нечетные простые числа и $y \in QR_n$. Тогда четыре корня числа y обладают следующими свойствами:

1) все они отличаются друг от друга;

2) $x_1 + x_4 = x_2 + x_3 = n$.

Криптосистема Рабина

Криптосистема, разработанная Рабином (Rabin), основана на сложности вычисления квадратного корня по модулю составного числа.

Стойкость этой криптосистемы эквивалентна неразрешимости задачи разложения целых чисел на множители. Алгоритм шифрования чрезвычайно эффективен и пригоден для многих практических приложений, например, для шифрования с помощью портативных устройств.

Выбираем два простых числа p и q, удовлетворяющих условию $|p| \approx |q|$, $n = p \cdot q$.

Выбираем число $b \in Z/nZ^*$.

Используем пару (n, b) в качестве параметров открытого ключа и запоминаем пару (p, q) в качестве параметров закрытого ключа.

Шифрование

Для того, чтобы послать секретное сообщение $m \in Z/nZ^*$, создаем зашифрованный текст

$$c \equiv m(m+b) (\mathrm{mod}\, n).$$

Расшифровка

Для того чтобы расшифровать текст c, нужно решить квадратное уравнение

$$m^2 + bm - c \equiv 0 \ (\mathrm{mod}\, n), \text{ где } m < n.$$

Общее решение квадратного уравнения имеет вид:

$$m \equiv \frac{-b + \sqrt{\Delta_c}}{2} \ (\mathrm{mod}\, n), \text{ где } \Delta_c \overset{def}{=} b^2 + 4c (\mathrm{mod}\, n).$$

Поскольку число c зависит от элемента $m \in Z/nZ^*$, квадратное уравнение $m^2 + bm - c \equiv 0 (\mathrm{mod}\, n)$ имеет решения в Z/nZ^*. Одним из этих решений является число m. Отсюда следует, что число Δ_c должно быть квадратичным вычетом по модулю n, т. е. элементом группы QR_n.

Вычисления, связанные с расшифровкой, содержат операцию извлечения квадратного корня по модулю n. Для каждого зашифрованного текста существует четыре разных значения $\sqrt{\Delta_c}$, и, следовательно, существует четыре разных результата шифрования. Как правило, реальное исходное сообщение содержит

избыточную информацию (*redundant information*), позволяющую отличить правильные тексты от неправильных.

Если число n является целым числом Блюма (*Blum integer*), т. е. $n = p \cdot q$, где $p \equiv q \equiv 3(\mathrm{mod}\,4)$, вычисление квадратных корней по модулю n сводится к вычислению квадратных корней по модулю p и q с помощью алгоритма для $p \equiv 3,7(\mathrm{mod}\,8)$ и применения китайской теоремы об остатках.

Пример 6.2. Шифрование.

Выбираем числа $p = 11$, $q = 19$, $n = 11 \cdot 19 = 209$ и $b = 183$.

Объявляем пару $(n, b) = (209, 183)$ параметрами открытого ключа криптосистемы Рабина. Зашифруем исходное сообщение $m = 31$.

$$c = 31 \cdot (31 + 183) = 155(\mathrm{mod}\,209).$$

Результирующий зашифрованный текст равен 155.

Пример 6.3. Расшифровка.

Для расшифровки этого сообщения вычисляем величину $\Delta_c = b^2 + 4c = 183^2 + 4 \cdot 155 \equiv 42(\mathrm{mod}\,209)$.

Теперь определим четыре корня числа 42 по модулю 209:

$$x_{11} = \sqrt{42(\mathrm{mod}11)},$$

$$x_{19} = \sqrt{42(\mathrm{mod}19)},$$

$$p = 11 \equiv 3(\mathrm{mod}8),$$

$$x_{11} = 42^{\frac{1+11}{4}}(\mathrm{mod}11) \equiv 3(\mathrm{mod}11),$$

$$q = 19 \equiv 3(\mathrm{mod}8),$$

$$x_{19} = 42^{\frac{1+19}{4}}(\mathrm{mod}19) \equiv 17(\mathrm{mod}19).$$

Найдем один из корней:

$$\begin{cases} x_1 = 3 (\mathrm{mod} 11) \\ x_1 = 17 (\mathrm{mod} 19) \end{cases},$$

$$11^{-1} (\mathrm{mod} 19) \equiv 7.$$

Далее воспользуемся формулой Гарнера:

$$x_1 = \left(14 \cdot 7 \left(\mathrm{mod} 19\right)\right) \cdot 11 + 3 = 36.$$

Приступим к отысканию следующего корня:

$$q - x_q = 19 - 17 = 2,$$

$$\begin{cases} x_2 = 3 (\mathrm{mod} 11) \\ x_2 = 2 (\mathrm{mod} 19) \end{cases},$$

$$x_2 = \left(\left((2-3)\left(11^{-1} \mathrm{mod} 19\right)\right) \mathrm{mod} 19\right) \cdot 11 + 3 = 12 \cdot 11 + 3 = 135.$$

Остальные корни находим по теореме 6.4:

$$36 + x_4 = 135 + x_3 = 209.$$

Значит $x_3 = 74$ и $x_4 = 173$.

Теперь ищем четыре варианта зашифрованного сообщения:

$$m_1 = \frac{-183 + 36}{2} (\mathrm{mod}\, 209) \equiv \frac{-147 + 209}{2} (\mathrm{mod}\, 209) \equiv 31,$$

$$m_2 = \frac{-183 + 135}{2} (\mathrm{mod}\, 209) \equiv -24 (\mathrm{mod}\, 209) \equiv 185,$$

$$m_3 = \frac{-183 + 74}{2} (\mathrm{mod}\, 209) \equiv \frac{-109 + 209}{2} (\mathrm{mod}\, 209) \equiv 50,$$

$$m_4 = \frac{-183 + 173}{2} (\mathrm{mod}\, 209) = -5 (\mathrm{mod}\, 209) \equiv 204.$$

Один из вариантов – наше сообщение 31!

Задания для аудиторной работы

Задание 1. Зашифровать в системе Рабина слово «Ор».

Решение. Цифровым аналогом этого слова будет число $m = 1618$.

Возьмем два числа Блюма $p = 43$ и $q = 47$, $n = p \cdot q = 43 \cdot 47 = 2021$.

Проверим, что $1618 \in Z/2021Z^*$.

Выбираем $b = 15$, принадлежащее $Z/2021Z^*$.

Тогда отправляемое сообщение

$$c = m \cdot (m + b) = 1618(1618 + 15) = 2642194 \pmod{2021} \equiv 747.$$

Передаваемое сообщение $(747, 2021, 15)$.

Задание 2. Расшифровать сообщение $(747, 2021, 15)$.

Решение. Найдем $\Delta_c = b^2 + 4c = 3213 \pmod{2021} \equiv 1192$,

$$x_{43} = \sqrt{1192 \pmod{43}},$$

$$x_{47} = \sqrt{1192 \pmod{47}},$$

$$x_{43} = 1192^{\frac{43+1}{4}} \pmod{43} = 1192^{11} \pmod{43}.$$

$$11 = 8 + 2 + 1,$$

$$1192 \pmod{43} \equiv 31,$$

$$1192^2 \equiv 31^2 \pmod{43} \equiv 15,$$

$$1192^4 \equiv 15^2 \pmod{43} \equiv 10,$$

$$1192^8 \equiv 10^2 \pmod{43} \equiv 14,$$

$$1192^{11} \equiv 14 \cdot 15 \cdot 31 \pmod{43} \equiv 17,$$

$$x_{43} = 17,$$

$$x_{47} = 1192^{\frac{47+1}{4}} = 1192^{12} \pmod{47},$$

$$12 = 8 + 4,$$

$$1192 \equiv 17 \pmod{47},$$

$$1192^2 \equiv 17^2 \pmod{47} \equiv 7,$$

$$1192^4 \equiv 7^2 \pmod{47} \equiv 49,$$

$$1192^8 \equiv 49^2 \pmod{47} \equiv 4,$$

$$1192^{12} \equiv 4 \cdot 49 \pmod{47} \equiv 8,$$

$$x_1 = \begin{cases} 17 \pmod{43} \\ 8 \pmod{47} \end{cases},$$

$$47^{-1} \pmod{43} = 11,$$

$$x_1 = \left(\left((17-8)\left(47^{-1} \bmod 43\right) \bmod 43\right)\right) \cdot 47 + 8 = \left(9 \cdot 11 \bmod 43\right) \cdot 47 + 8 = 13 \cdot 47 + 8 = 619,$$

$$x_2 = \begin{cases} 17 \pmod{43} \\ (47-8) \pmod{47} \end{cases} = \begin{cases} 17 \pmod{43} \\ 39 \pmod{47} \end{cases},$$

$$x_2 = \left(\left((17-39)\left(47^{-1} \bmod 43\right)\right) \bmod 43\right) \cdot 47 + 39 = \left((-22 \cdot 11) \bmod 43\right) \cdot 47 + 39 =$$
$$= 16 \cdot 47 + 39 = 791,$$

$$619 + x_4 = 791 + x_3 = 2021,$$

$$x_4 = 1402, \quad x_3 = 1230.$$

Таким образом, мы нашли четыре квадратных корня числа 1192 по модулю 2021.

Приступим к следующему этапу расшифровки и найдем четыре варианта зашифрованного сообщения:

$$m_1 = \frac{-15 + 619}{2} \pmod{2021} \equiv 302,$$

$$m_2 = \frac{-15 + 791}{2} \pmod{2021} \equiv 388,$$

$$m_3 = \frac{-15 + 1230}{2} \pmod{2021} \equiv \frac{1215 + 2021}{2} \pmod{2021} \equiv 1618,$$

$$m_4 = \frac{-15 + 1402}{2} \pmod{2021} \equiv \frac{1387 + 2021}{2} \pmod{2021} \equiv 1704.$$

Один из вариантов $m_3 = 1618$ – наше сообщение, цифровой аналог слова «Ор».

Индивидуальные задания

Расшифровать сообщение (криптосистема Рабина).

Вариант 1

$c = 94,\ n = 589,\ b = 20.$

Вариант 2

$c = 373,\ n = 713,\ b = 25.$

Вариант 3

$c = 1795,\ n = 1817,\ b = 13.$

Вариант 4

$c = 214,\ n = 1633,\ b = 17.$

Вариант 5

$c = 1923,\ n = 2881,\ b = 12.$

Вариант 6

$c = 1317,\ n = 1349,\ b = 18.$

Вариант 7

$c = 1535,\ n = 2201,\ b = 21.$

Вариант 8

$c = 850,\ n = 1829,\ b = 22.$

Вариант 9

$c = 1032,\ n = 2773,\ b = 27.$

Вариант 10

$c = 68,\ n = 2537,\ b = 15.$

Вариант 11

$c = 1220,\ n = 2881,\ b = 33.$

Вариант 12

$c = 27,\ n = 253,\ b = 50.$

Вариант 13

$c = 1121,\ n = 1457,\ b = 40.$

Вариант 14

$c = 48,\ n = 341,\ b = 72.$

Вариант 15

$c = 1829,\ n = 4757,\ b = 26.$

Лабораторная работа № 7
CRIPTOSYSTEM EL GAMAL

Цель работы: изучение шифрования с помощью криптосистемы El Gamal.

Необходимые теоретические сведения

Криптосистема Эль Гамаля

Криптосистема Эль Гамаля создана американским специалистом по криптографии в 1985 году после появления криптосистемы *RSA*. Она послужила основой для целого ряда систем цифровой подписи, в том числе российской и белорусской.

Криптосистема Эль Гамаля строится на основе большого простого числа $p \approx 2^q$, где $512 \le q \le 1024$, то есть имеющее 150–300 десятичных знаков. Кольцо классов вычетов $Z/pZ = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{p-1}\}$ в силу простоты числа p обладает тем свойством, что все ненулевые классы в нем обратимы относительно умножения. В дальнейшем нам понадобится следующая теорема.

Теорема 7.1. Для всякого простого числа p мультипликативная группа Z/pZ^* является циклической.

Вернемся к изложению криптосистемыЭль Гамаля. Пусть $\overline{g}$ – фиксированный примитивный элемент поля Z/pZ – образующая циклической группы Z/pZ^*. Это означает, что степени $\overline{g}$ как элемента группы Z/pZ^* исчерпывают всю эту группу. Иными словами, мультипликативная подгруппа $< \overline{g} >$ совпадает со всей группой: $< \overline{g} >= \{\overline{g}, \overline{g}^2, ..., \overline{g}^{p-1} = 1\} = Z/pZ^*$.

В дальнейшем $\overline{g}$ рассматриваем как обычное натуральное число $g < p$. Фиксируем два секретных ключа x и k как элементы Z/pZ^*. При этом x знают пользователи на обоих концах криптосистемы, а k – это сеансовый ключ, выбираемый отправителем на короткий промежуток работы системы – один или

несколько сеансов передачи информации. Отправитель вычисляет величину $y = g^x (\mathrm{mod}\, p)$. Тройка чисел (p, g, y) – есть тройка открытых ключей криптосистемы Эль Гамаля.

Передаваемая информация в криптосистеме Эль Гамаля, как и в криптосистеме *RSA*, предварительно преобразуется в десятичное число – сообщение $\bar{c}$, рассматриваемое как элемент группы Z/pZ^*. Сообщение шифруется умножением $\bar{c}$ на $K = y^k (\mathrm{mod}\, p)$. Таким образом, зашифрованное сообщение $\overline{m} = \bar{c} \cdot K (\mathrm{mod}\, p) = \bar{c} \cdot y^k (\mathrm{mod}\, p)$. При этом адресату идет расширенное сообщение: $(\overline{m}, O_{CK})$, где $O_{CK} = g^k (\mathrm{mod}\, p)$ – число-подсказка, называемое открытым сеансовым ключом.

Получатель послания знает секретный ключ x. Он возводит O_{CK} в степень x по модулю p: $O_{CK}^x = g^{kx} (\mathrm{mod}\, p) = (g^x)^k (\mathrm{mod}\, p) = y^k (\mathrm{mod}\, p) = K$. Вычислив K, получатель находит K^{-1} в кольце Z/pZ. Это несложно сделать, например, обратной прогонкой алгоритма Евклида с учетом соотношения $\mathrm{НОД}(K, p) = 1$. Теперь сообщение легко восстанавливается: $\overline{m} \cdot K^{-1} (\mathrm{mod}\, p) = \bar{c}$.

Проблема взлома данной криптосистемы подкупающе проста: надо найти x – степень числа g по модулю p, равную y. Это так называемая проблема дискретного логарифма. Приемлемых решений этой проблемы, кроме прямого последовательного перебора степеней g по модулю p до искомой на сегодняшний день не существует.

Пример 7.1. Пусть $p = 23$. Вычисления показывают, что в качестве g можно взять число 5. Положим в качестве секретного ключа число $x = 7$. Тогда стандартными вычислениями находим третий открытый ключ y:

$$y = g^x (\mathrm{mod}\, p) = 5^7 (\mathrm{mod}\, 23) \equiv 5^2 \cdot 5^2 \cdot 5^2 \cdot 5 (\mathrm{mod}\, 23) \equiv$$

$$\equiv 2 \cdot 2 \cdot 2 \cdot 5 (\mathrm{mod}\, 23) \equiv 40 (\mathrm{mod}\, 23) \equiv 17.$$

В качестве секретного сеансового ключа возьмем $K = 3$. В таком случае можно вычислить $K = y^k (\mathrm{mod}\, p) = 17^3 (\mathrm{mod}\, 23) \equiv 289 \cdot 17 (\mathrm{mod}\, 23) \equiv 13 \cdot 17 (\mathrm{mod}\, 23) \equiv 14.$

Тогда $O_{СК} = g^k \pmod p = 5^3 \pmod{23} \equiv 10$. Криптосистема Эль Гамаля полностью подготовлена к работе.

Предположим, что передается сообщение $\bar{c} = 20$. Тогда шифровка $\overline{\overline{m}} = \bar{c} \cdot K \pmod p = 20 \cdot 14 \pmod{23} = 4$. Следовательно, адресат получает сообщение $(\overline{\overline{m}}, O_{СК}) = (4, 10)$. Напомним, что у него в распоряжении имеется тройка открытых ключей $(p, g, y) = (23, 5, 17)$ и секретный ключ $x = 7$.

Получатель знает секретный ключ x. Для расшифровки принятого сообщения он вычисляет

$$K = O_{СК}^x = g^{kx} \pmod p = 10^7 \pmod{23} = 8 \cdot 8 \cdot 8 \cdot 10 \pmod{23} = 18 \cdot 11 \pmod{23} = 14.$$

Затем получатель находит в кольце $Z/23Z$ $K^{-1} = 5$ и, наконец, вычисляет правильное сообщение: $\bar{c} = 4 \cdot 5 = 20$.

Взломщику для расшифровки этого же сообщения необходимо найти x. Для этого ему придется последовательно перебирать степени g до тех пор, пока не получит y. Эту работу можно рассматривать как частичное восстановление циклической группы $< g >= \{g, g^2, ..., g^x = y, ...\}$. В данном случае фрагмент группы $< g = 5 >= \{5, 2, 10, 4, 20, 8, 17 = y\}$. Отсюда следует, что $x = 7$. Конечно, в реальной ситуации x столь малым не будет: в его вычислении и содержится, как уже отмечалось, вся криптостойкость системы Эль Гамаля. Вычислив x, взломщик сможет без особого труда повторить операции получателя по расшифровке сообщения.

Задания для аудиторной работы

Задание 7.1. Зашифруйте по схеме Эль Гамаля слово «ау».

Решение неоднозначно. Естественно, переход от слова к числу осуществим, как и в схеме *RSA*: $a \leftrightarrow 01$, $y \leftrightarrow 21$. Поэтому $ay \leftrightarrow 121$. Итак сообщение $c = 121$. Ближайшее большее простое число – 127. Это четвертое из списка знаменитых простых чисел Мерсена: $127 = 2^7 - 1$. Известно, что здесь в качестве g можно

взять число $g=3$. Выберем секретные ключи x и k. К примеру, возьмем $x=37$, а $k=14$. Теперь необходимо вычислить $y=g^x(\mathrm{mod}\,p)$. Не имея компьютера под рукой, проведем эти вычисления вручную:

$g^2=9,\ g^4=9^2=81,$

$g^8=81^2=6561\equiv 84(\mathrm{mod}127),$

$g^{16}=84^2=7056\equiv 71(\mathrm{mod}127).\ g^{32}=71^2=5041\equiv 88(\mathrm{mod}127).$

Следовательно, $g^{37}=g^{32+4+1}\equiv 88\cdot 81\cdot 3(\mathrm{mod}127)\equiv 810(\mathrm{mod}127)=48(\mathrm{mod}127).$ Таким образом, $y=48$.

Теперь вычислим шифрующий множитель $K=y^k(\mathrm{mod}\,p)$. Для этого вновь необходимо найти серию степеней: $y^2=2304\equiv 18(\mathrm{mod}127)$, $y^4\equiv 70(\mathrm{mod}127)$, $y^8\equiv 74(\mathrm{mod}127)$. Поэтому

$y^{14}\equiv 74\cdot 70\cdot 18(\mathrm{mod}127)\equiv 100\cdot 18(\mathrm{mod}127)\equiv 22(\mathrm{mod}127).$

Таким образом, $K=22$.

$ш=c\cdot K(\mathrm{mod}\,p)=121\cdot 22(\mathrm{mod}127)\equiv 122(\mathrm{mod}127)$. Итак, $ш=122$.

Осталось вычислить открытый сеансовый ключ $O_{CK}=g^k(\mathrm{mod}\,p)=3^{14}(\mathrm{mod}127)$. Учитывая проведенные выше утверждения, имеем $O_{CK}=84\cdot 81\cdot 9(\mathrm{mod}127)\equiv 22(\mathrm{mod}127)$. Итак, $O_{CK}=22$.

Зашифрованное по схеме Эль Гамаля сообщение построено: $(p,g,y,ш,O_{CK})=(127,\ 3,\ 48,\ 122,\ 22)$.

Задание 7.2. Находясь в роли получателя, расшифруйте сообщение $(p,\ g,\ y,\ ш,\ O_{CK})=(127,\ 3,\ 48,\ 122,\ 22)$, зашифрованное по схеме Эль Гамаля. Вам известен также секретный ключ $x=37$.

Решение. Получатель вычисляет $O_{CK}^x=22^{37}(\mathrm{mod}127)=K$. $O_{CK}^2=22^2\equiv 103(\mathrm{mod}127)$. $O_{CK}^4=68(\mathrm{mod}127)$. $O_{CK}^8=52$. $O_{CK}^{16}=37$. $O_{CK}^{32}=37^2=1369\equiv 99(\mathrm{mod}127)$. Следовательно, $K=22^{37}(\mathrm{mod}127)=99\cdot 68\cdot 22=22$ по модулю 127.

Теперь вычислим K^{-1} в кольце $Z/127Z$ с помощью расширенного алгоритма Евклида.

$127 = 22 \cdot 5 + 17$. $22 = 17 \cdot 1 + 5$. $17 = 5 \cdot 3 + 2$. $5 = 2 \cdot 2 + 1$. НОД$(127, 22) = 1$.

Построим соотношение Безу для чисел 127 и 22.

$$1 = 5 + 2 \cdot (-2) = 5 + (-2) \cdot [17 + 5 \cdot (-3)] = 5 \cdot 7 + 17 \cdot (-2) = 7 \cdot [22 + 17 \cdot (-1)] + 17 \cdot (-2) =$$
$$= 22 \cdot 7 + 17 \cdot (-9) = 22 \cdot 7 + (-9) \cdot [127 + 22 \cdot (-5)] = 22 \cdot 52 + 127 \cdot (-9) = 1.$$

Из построенного соотношения Безу следует, что $K^{-1} = 52$. Расшифровка состоит в вычислении произведения $ш \cdot K^{-1} (\mathrm{mod}\, p) = 122 \cdot 52 (\mathrm{mod} 127) = 121$. Таким образом, принято сообщение «Ау».

Задание 7.3. В роли несанкционированного пользователя, не зная секретного ключа x, попытайтесь «взломать» (расшифровать) сообщение $(p, g, y, ш, O_{СК}) = (127, 3, 48, 122, 22)$.

Решение. Построим фрагмент циклической группы $\langle g \rangle = \langle 3 \rangle = \{3, 3^2 = 9, \ldots\}$ до получения равенства $3^x = 48$. Найдя таким образом x, далее повторим вычисления, проведенные в решении задания 7.2.

Индивидуальные задания

Расшифровать перехваченную криптосистему Эль Гамаля.

Вариант 1

а) p = 23; g = 5; y = 10; $O_{СК}$ = 8; $ш$ = 21.

б) $ш$ = 160936054; $O_{СК}$ = 1449464; y = 57348448; p = 206181067; g = 7.

Вариант 2

а) p = 211; g = 2; y = 8; $O_{СК}$ = 64; $ш$ = 170.

б) $ш$ = 125176846; $O_{СК}$ = 93916858; y = 44618890; p = 218012117; g = 2.

Вариант 3

а) $p = 211$; $g = 2$; $y = 8$; $O_{СК} = 64$; $ш = 52$.

б) $ш = 102541510$; $O_{СК} = 4532899$; $y = 189617901$; $p = 221151019$; $g = 11$.

Вариант 4

а) $p = 3307$; $g = 2$; $y = 8$; $O_{СК} = 64$; $ш = 1525$.

б) $ш = 281533687$; $O_{СК} = 110361597$; $y = 57882185$; $p = 310241023$; $g = 5$.

Вариант 5

а) $p = 1621$; $g = 2$; $y = 8$; $O_{СК} = 64$; $ш = 1374$.

б) $ш = 17960572$; $O_{СК} = 262582374$; $y = 349975032$; $p = 401132107$; $g = 5$.

Вариант 6

а) $p = 11239$; $g = 3$; $y = 27$; $O_{СК} = 729$; $ш = 3158$.

б) $ш = 166161904$; $O_{СК} = 166506866$; $y = 102149179$; $p = 401141729$; $g = 6$.

Вариант 7

а) $p = 521$; $g = 3$; $y = 27$; $O_{СК} = 208$; $ш = 42$.

б) $ш = 65214599$; $O_{СК} = 340504920$; $y = 293459573$; $p = 401150527$; $g = 3$.

Вариант 8

а) $p = 719$; $g = 11$; $y = 612$; $O_{СК} = 664$; $ш = 270$.

б) $ш = 112631540$; $O_{СК} = 43358355$; $y = 38141939$; $p = 406112029$; $g = 2$.

Вариант 9

а) $p = 2203$; $g = 5$; $y = 125$; $O_{СК} = 204$; $ш = 1396$.

б) $ш = 131187373$; $O_{СК} = 65043717$; $y = 82746985$; $p = 406181621$; $g = 3$.

Вариант 10

а) $p = 127$; $g = 3$; $y = 27$; $O_{СК} = 94$; $ш = 91$.

б) $ш = 352830981$; $O_{СК} = 4226565$; $y = 369353956$; $p = 416020247$; $g = 5$.

Вариант 11

а) $p = 503$; $g = 5$; $y = 125$; $O_{СК} = 32$; $ш = 357$.

б) $ш = 291880466$; $O_{СК} = 366156037$; $y = 350826080$; $p = 418101419$; $g = 2$.

Вариант 12

а) $p = 1811$; $g = 6$; $y = 216$; $O_{СК} = 1381$; $ш = 1158$.

б) $ш = 161375365$; $O_{СК} = 350245652$; $y = 324780822$; $p = 507151027$; $g = 2$.

Вариант 13

а) $p = 1847$; $g = 5$; $y = 125$; $O_{СК} = 849$; $ш = 1791$.

б) $ш = 91384391$; $O_{СК} = 379249718$; $y = 101728180$; $p = 516111331$; $g = 2$.

Вариант 14

а) $p = 1423$; $g = 3$; $y = 27$; $O_{СК} = 729$; $ш = 233$.

б) $ш = 508050716$; $O_{СК} = 208855653$; $y = 691205734$; $p = 821121611$; $g = 2$.

Вариант 15

а) $p = 1361$; $g = 3$; $y = 27$; $O_{СК} = 729$; $ш = 592$.

б) $ш = 214671795$; $O_{СК} = 1209262383$; $y = 528288046$; $p = 1216150609$; $g = 13$.

ЛИТЕРАТУРА

1. Белоногов В.А. Задачник по теории групп / В.А. Белоногов. – М: Наука, 2000. – 239 с.

2. Биркгоф Г. Современная прикладная алгебра / Г. Биркгоф, Т. Барти. – М.: Мир, 1976. – 400 с.

3. Виноградов И.М. Основы теории чисел / И.М. Виноградов. – М.: Наука, 1982. – 168 с.

4. Горчаков Ю.М. Теория групп: учебное пособие / Ю.М. Горчаков. – Тверь: Тверской гос. ун-т, 2002. – 114 с.

5. Липницкий В.А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа: учебно-методическое пособие / В.А. Липницкий. – 2-е изд. – Минск, 2006. – 88 с.

6. Практические и лабораторные занятия по курсу «Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа»: учебно-методическое пособие / В.А. Липницкий [и др.]. – Минск: БГУИР, 2006. – 70 с.

7. Нечаев В.И. Элементы криптографии. Основы теории защиты информации / В.И. Нечаев. – М.: Высшая школа, 1999. – 110 с.

8. Холл М. Теория групп / М. Холл. – М.: ИЛ, 1962. – 468 с.

9. Мао В. Современная криптография: теория и практика / В. Мао. – М.: Вильямс. – 2005. – 768 с.

10. Фергюсон Н. Практическая криптография / Н. Фергюсон, Б. Шнайдер. – М.: Вильямс, 2005. – 424 с.