МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

«АЛТАЙСКАЯ ГОСУДАРСТВЕННАЯ ПЕДАГОГИЧЕСКАЯ АКАДЕМИЯ»

Курсовая работа

по дисциплине «Алгебра»

Китайская Теорема об остатках и её следствия

Выполнила студентка

группы

Станевич Маргарита

Научный руководитель

Мальцев Ю.Н

Барнаул 2013

**Оглавление**

Введение

Глава 1. Элементарная теория сравнений, а ≡ b (mod p)

. Определения и основные свойства сравнений

. Теорема Эйлера, теорема Ферма

Глава 2. Китайская теорема об остатках

. Китайская теорема об остатках (КТО)

. Примеры. Применение к решению олимпиадных задач

. КТО. Применение к открытию сейфа в банке

Заключение

Список литературы

**Введение**

Первоначальные элементы математики связаны с появлением навыков счета, возникающих в примитивной форме на сравнительно ранних ступенях развития человеческого общества в процессе трудовой деятельности. Понятие натурального числа, появляющееся как результат постепенного абстрагирования, является основой всего дальнейшего развития математики. В теории чисел, естественно, выделяются и рассматриваются в первую очередь те проблемы, которые глубоко и достаточно непосредственно связаны с изучаемыми объектами и важны для построения математики в ее целом. Некоторые теоретико-числовые задачи возникают уже в рамках школьного курса арифметики. Исторически теория чисел возникла как непосредственное развитие арифметики. В настоящее время в теорию чисел включают значительно более широкий круг вопросов, выходящих за рамки изучения натуральных чисел. В теории чисел рассматриваются не только натуральные числа, но и множество всех целых чисел, а также множество рациональных чисел.

Современную теорию чисел можно в основном разбить на следующие разделы:

) Элементарная теория чисел (теория сравнений, теория форм, неопределенные уравнения). К этому разделу относят вопросы теории чисел, являющиеся непосредственным развитием теории делимости, и вопросы о представимости чисел в определенной форме. Более общей является задача решения систем неопределенных уравнений, т. е. уравнений, в которых значения неизвестных должны быть обязательно целыми числами. Неопределенные уравнения называют также диофантовыми уравнениями, так как Диофант был первым математиком, систематически рассматривавшим такие уравнения. Мы условно называем этот раздел „Элементарная теория чисел", поскольку здесь часто применяются обычные арифметические и алгебраические методы исследования.

) Алгебраическая теория чисел. К этому разделу относят вопросы, связанные с изучением различных классов алгебраических чисел.

) Диофантовы приближения. К этому разделу относят вопросы, связанные с изучением приближения действительных чисел рациональными дробями. К диофантовым приближениям примыкают тесно связанные с этим же кругом идей вопросы изучения арифметической природы различных классов чисел.

) Аналитическая теория чисел. К этому разделу относят вопросы теории чисел, для изучения которых приходится применять методы математического анализа.

В данной курсовой работе мы столкнемся с элементарной теорией чисел, а точнее с элементарной теорией сравнений, её основными свойствами и определениями, которые будут рассмотрены в первой главе.

Во второй главе будет рассмотрен один из важных результатов теории чисел, так называемая китайская теорема об остатках (KTO). По существу эта теорема утверждает, что можно восстановить целое число по множеству его остатков от деления на числа из некоторого набора попарно взаимно простых чисел. Эта теорема в её арифметической формулировке была описана в трактате китайского математика Сунь Цзы «Сунь Цзы Суань Цзин» (кит.упр.孙子算经, пиньинь: sunzi suanjing), предположительно датируемом третьим веком н. э. и затем была обобщена Цинь Цзюшао в его книге «Математические рассуждения в 9 главах» датируемой 1247 годом.

Китайская теорема об остатках широко применяется в теории чисел, криптографии и других дисциплинах:

. Взаимно однозначное соответствие между некоторым числом и набором его остатков, определяемым набором взаимно простых чисел, существование которого утверждается в теореме, на практике помогает работать не с длинными числами, а с наборами их коротких по длине остатков. Кроме того вычисления по каждому из модулей можно выполнять параллельно. Если в качестве базиса взять, к примеру, первые 500 простых чисел, длина каждого из которых не превосходит 12 бит, то этого хватит для представления десятичных чисел длиной до 1519 знаков. (Откуда взялось число 1519 понять очень просто: сумма десятичных логарифмов первых 500 простых чисел равна 1519,746…). Например, в алгоритме RSA вычисления производятся по модулю очень большого числа n, представимого в виде произведения двух больших простых чисел. Теорема позволяет перейти к вычислениям по модулю этих простых делителей, которые по величине уже порядка корня из n, а значит имеют в два раза меньшую битовую длину. Отметим также, что применение вычислений согласно китайской теореме об остатках делает алгоритм RSA восприимчивым к атакам по времени.

. На теореме основаны схема Асмута - Блума и схема Миньотта - пороговые схемы разделения секрета в группе участников. Секрет могут узнать только k из n участников, объединив свои ключи.

. Одним из применения является быстрое преобразование Фурье на основе простых чисел

. Теорема лежит в основе принципа Хассе поиска целочисленных корней уравнения.

. Из теоремы следует мультипликативность функции Эйлера.

. На теореме основывается алгоритм Полига-Хеллмана нахождения дискретного логарифма за полиномиальное время для чисел, имеющих специальный вид.

. Теорема имеет множество применений в шифровании и дешифровании в криптографических системах, например, в криптосистеме Рабина или в шифре Виженера.

**Глава 1. Элементарная теория сравнений, а ≡ b (mod p)**

**. Определения и основные свойства сравнений**

В данном параграфе мы рассмотрим целые числа, а обозначать их будем латинскими буквами.

Возьмём произвольное фиксированное натуральное число p и будем рассматривать остатки при делении на р различных целых чисел.

При рассмотрении свойств этих остатков и проведении операций над ними удобно ввести понятие сравнения по модулю.

**Определение**. Целые числа а и b называются сравнимыми по модулю р, если разность чисел а - b делится на р, то есть, если . Таким образом сравнение представляет собой соотношение между тремя числами a,b и p, причем p,играющее своего рода эталона сравнения, мы называем модулем. Для краткости мы будем это соотношение между a, b и p записывать следующим образом: a≡b (mod p), a и b будем называть соответственно левой и правой частями сравнения. Число p, стоящее под знаком модуля, будем всегда считать положительным, т.е запись mod p будет означать, что, числа а и b - вычеты. Если разность а - b не делится на р, то а не сравнимо с b по mod p.

Согласно определению а ≡ 0 (mod p) означает, что а делится на р.

Пример:

≡ 17 (mod 21)т. к. 101 - 17 = 84, а 84⁞21.

**Теорема:** число а сравнимо с числом b по модулю p тогда и только тогда, когда а и b имеют одинаковые остатки при делении на р, поэтому в качестве определения сравнения можно взять следующее:

**Определение:** Целые числа а и b называются сравнимыми по модулю р, если остатки от деления этих чисел на р равны.

Дадим **основные свойства сравнений:**

. Рефлексивность отношения сравнимости: а ≡ a (mod p)

.Симметричность отношения сравнимости:

если, а ≡ b (mod p) то b ≡ a (mod p).

3. Транзитивность отношения сравнимости:

если а ≡ b (mod p), b ≡ c (mod p), то а ≡ c(mod p).

. Если а ≡ b (mod p) и k - произвольное целое число, то kа ≡ kb (mod p)

. Если kа ≡ kb (mod p) и (k, p) = 1, то а ≡ b (mod p).

. Если а ≡ b (mod p)и k- произвольное натуральное число, то kа ≡ kb (mod kp)

. Если kа ≡ kb (mod kp), где k и р - произвольные натуральные числа, то а ≡ b (mod p)

. Если а ≡ b (mod p),c ≡ d (mod p), то а+c ≡ b+d (mod p)и а-c ≡ b-d (mod p).

. Если а ≡ b (mod p), c ≡ d (mod p), то аc ≡ bd (mod p)

. Если а ≡ b (mod p), то при любом целом n > 0,а ≡ b (mod p).

. Если а ≡ b (mod p) и f(x)= +++... - произвольный многочлен с целыми коэффициентами, то f(а) ≡ f(b) (mod p)

. Любое слагаемое левой или правой части сравнения можно перенести с противоположным знаком в другую часть.

. Если а ≡ b (mod p) и , то а ≡ b (mod d)

. Если а ≡ b (mod p), то множество общих делителей а и р совпадает с множеством общих делителей b и р. В частности, (a,p)=(b,p).

. Если а ≡ b (mod ),а ≡ b (mod )…,а ≡ b (mod ), то а ≡ b (mod p), где p=[,,...,].

При делении целого числа на модуль р в остатке получается 0, 1, 2, 3,…,р- 1 чисел.

**2. Теорема Эйлера, теорема Ферма**

элементарный теорема китайский остаток

**Теорема (Эйлера).** Пусть m>1,(a,m)=1,j(m)- функция Эйлера. Тогда: aj(m)≡1(mod m)

**Доказательство.** Пусть х пробегает приведенную систему вычетов по mod m:

x=,,...,rc

где c=j(m) их число ,...,- наименьшие неотрицательные вычеты по mod m. Следовательно, наименьшие неотрицательные вычеты, соответствующие числам ax суть соответственно: - тоже пробегают приведенную систему вычетов, но в другом порядке. Значит:

a≡(mod m) a≡(mod m) ... arc≡ (mod m), c=φ(m)

Перемножим эти с штук сравнений. Получится:

≡ (mod m)

Так как ≠0 и взаимно просто с модулем m, то, поделив последнее сравнение на r1r2...rc, получим ).

**Теорема (Ферма).** Пусть р - простое число, р не делит a. Тогда: a p-1≡1(mod p).

**Доказательство 1.** Положим в условии теоремы Эйлера m=p, тогда φ (m)=p-1. Получаем.

**Замечание:** Необходимо отметить важность условия взаимной простоты модуля и числа a в формулировках теорем Эйлера и Ферма. Простой пример: сравнение  очевидно не выполняется.

Однако можно легко подправить формулировку теоремы Ферма, чтобы снять ограничение взаимной простоты.

**Глава 2. Китайская теорема об остатках**

**. Китайская теорема об остатках**

Одним из важных результатов теории чисел является так называемая китайская теорема об остатках (KTO). По существу эта теорема утверждает, что можно восстановить целое число по множеству его остатков от деления на числа из некоторого набора попарно взаимно простых чисел. Эта теорема в её арифметической формулировке была описана в трактате китайского математика Сунь Цзы «Сунь Цзы Суань Цзин» (кит.упр.孙子算经, пиньинь: sunzi suanjing), предположительно датируемом третьим веком н. э. и затем была обобщена Цинь Цзюшао в его книге «Математические рассуждения в 9 главах» датируемой 1247 годом, где было приведено точное решение.Существует несколько формулировок данной теоремы, я предоставлю здесь некоторые из них.

**Теорема.** Пусть , 1 ≤ i ≤ k, взаимно простые числа

и пусть ai целые числа. Тогда существует такое число x,

что имеет место

x≡ mod ,

x≡ ,

…

x≡ .

Наконец, рассмотрим еще одну формулировку теоремы,

которую будем использовать в практических работах.

**Теорема.** Пусть {} - взаимно простые числа и M = 

Пусть 0 ≤  ≤ , целые числа. Введем обозначение  = . Пусть  число, которое удовлетворяет сравнению ≡1 mod .При этих условиях сравнение

x≡ mod , имеет на интервале [0, M - 1] единственное решение,которое определяется формулой x =  + + … + 

В рамках условий теоремы китайская теорема об остатках утверждает, что существует взаимно однозначное соответствие между целыми числами и некоторым наборами целых чисел. Другими словами, для каждого целого числа B найдется соответствующий ему единственный набор чисел и наоборот, для каждого набора чисел () найдется единственное соответствующему этому набору число B.

**Арифметическая формулировка КТО:**

Если числа попарно взаимно просты, то для любых остатков таких, что при всех i= 1,2,...n., найдётся число N, которое при делении на даёт остаток при всех i= 1,2,...n.

**Доказательство:**

Применим индукцию по n. При n=1 утверждение теоремы очевидно. Пусть теорема справедлива при n= k-1, т. е. существует число M, дающее остаток при делении на при .Обозначим и рассмотрим числа . Покажем, что хотя бы одно из этих чисел даёт остаток при делении на . Допустим это не так. Поскольку количество чисел равно , а возможных остатков при делении этих чисел на может быть не более чем (ведь ни одно число не даёт остаток ), то среди них найдутся два числа, имеющих равные остатки (принцип Дирихле). Пусть это числа и при и . Тогда их разность делится на , что невозможно, т.к. и взаимно просто с , ибо числа попарно взаимно просты (по условию). Противоречие.

Таким образом, среди рассматриваемых чисел найдётся число , которое при делении на даёт остаток . В то же время при делении на число N даёт остатки соответственно.

**Наиболее используемая формулировка КТО:**

Пусть - попарно взаимно простые числа и - произвольные целые числа. Тогда существует целое число ,такое что Целое число у удовлетворяет условию  тогда и только тогда когда

**Доказательство**: Обозначим М=и . Тогда числа  являются взаимно простыми для всех i. Cледовательно существует целое число такое что  где . Положимтогда , поскольку числа . Аналогично доказывается, что . Пусть - остаток от деления числа a на M. Тогда и ≡ a (mod M). В частности  Далее, пусть целое чисто у удовлетворяет условию . Тогда т. е. Число делится на каждое из чисел .В силу того, что числа попарно взаимно простые, получаем что делится на число . Таким образом, ≡0 (mod ).Теорема доказана.

**2. Примеры. Применение к решению олимпиадных задач**

В этом параграфе я опишу один из методов решения систем линейных сравнений. Это очень древний алгоритм. Он применялся еще в античности для решения проблем астрономии. Приведу несколько примеров решения олимпиадных задач и примеров решения сравнений с помощью КТО. Начнем с задачи, сформулированной на современном языке, которая могла бы рассматриваться древними астрономами (Астрономический пример).

**Пример 1:** Три спутника пересекут меридиан города Лидса сегодня ночью: первый - в 1 ночи, второй - в 4 утра, а третий - в 8 утра. У каждого спутника свой период обращения. Первому на полный оборот вокруг Земли требуется 13 часов, второму - 15, а третьему - 19 часов. Сколько часов пройдет (от полуночи) до того момента, когда спутники одновременно пересекут меридиан Лидса?

Посмотрим, как эта задача переводится на язык сравнений.

Пусть х - количество часов, которые пройдут с 12 часов ночи до момента одновременного прохождения спутниками над меридианом Лидса. Первый спутник пересекает этот меридиан каждые 13 часов, начиная с часу ночи. Это можно записать

как х = 1 + 13t для некоторого целого t. Другими словами, х ≡ 1 (mod 13). Соответствующие уравнения для остальных спутников имеют вид: х ≡ 4 (mod 15) и х≡ 8 (mod 19). Таким образом, три спутника одновременно пересекут меридиан Лидса через х часов, если х удовлетворяет эти трем уравнениям. Следовательно, для ответа на поставленный вопрос достаточно решить систему сравнений:

х ≡ 1 (mod 13),

х ≡4 (mod 15), (B1)

х ≡ 8 (mod 19).

Заметим, что мы не можем складывать или вычитать уравнения системы, поскольку модули сравнений в них разные. Будем решать эту задачу, переходя от сравнений к уравнениям в целых числах. Так, сравнение х ≡ 1 (mod 13) соответствует диофантову уравнению: х = 1 + 13t. Заменяя х во втором сравнении системы на 1 + 13t, получаем:

+ 13t ≡ 4 (mod 15), т.е. 13t ≡ 3 (mod 15).

Но 13 обратимо по модулю 15, обратный к нему элемент - это 7. Умножая последнее сравнение на 7 и переходя в нем к вычетам по модулю 15, имеем:

t ≡ 6 (mod 15).

Значит, t может быть записан в виде: t = 6+15u для какого-то целого u. Следовательно,

х = 1 + 13t = 1 + 13(6 + 15u) = 79 + 195u.Заметим, что все числа вида 79 + 195u являются целыми решениями первых двух сравнений системы (B.1). Наконец, подставим в третье сравнение вместо х выражение 79 + 195u:

+ 195u ≡ 8 (mod 19), так что 5u ≡ 5 (mod 19).

Ввиду обратимости остатка 5 по модулю 19, на него можно сократить и увидеть, что

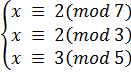
u ≡ 1 (mod 19). Переписывая это сравнение как диофантово уравнение, мы получим

u= 1 + 19v для некоторого целого v.

Итак, х = 79 + 195u = 79 + 195(1 + 19v) = 274 + 3705v.

Какой отсюда можно сделать вывод относительно спутников? Напомним, что х - количество часов, которые пройдут от полуночи до момента одновременного прохождения спутников над меридианом Лидса. Поэтому нам нужно было найти наименьшее натуральное значение переменной х, удовлетворяющее системе (B.1). Мы это сделали. Поскольку решение системы: х = 274 + 3705v, то ответ: 274. Итак, спутники одновременно пройдут над меридианом Лидса через 274 часа после 0 часов сегодняшней ночи, что соответствует 11 дням и 10 часам. Но общее решение системы дает больше информации. Прибавляя к 274 любое кратное 3705, мы получаем другое решение системы. Иначе говоря, спутники одновременно пересекают означенный меридиан каждые 3705 часов после первого такого момента, что соответствует 154 дням и 9 часам.

**Пример 2**: Найти все целые решения системы сравнений:



Решение: М= 3\*5\*7=105

Найдем целые числа ,,такие что :

1)\*35≡1 (mod 3) \*2≡1 (mod 3)

=-1(mod 3)

)\*21≡1 (mod 5) \*1≡1 (mod 5)

=1

)\*15≡1 (mod 7)

=1

По КТО:

≡,

подставим найденные нами значения в формулу:

≡-1\*35\*2+ 1\*21\*3+1\*15\*2=23, т. е.

Числа вида 23+105t, где ,исчерпывают все множество решений исходной системы сравнений.

Ответ: 23+105t.

**Пример 3**: Доказать что сравнение ≡ 0 (mod m)разрешимо для каждого натурально числа m>1, несмотря на то, что уравнение =0 не имеет целых решений.

Поскольку =(2x+1)(3x+1), то уравнение не имеет решений в кольце . Пусть m=(2b+1). тогда по китайской теореме об остатках существует целое число х, такое, что 3х≡ -1(mod) и 2х≡-1(mod(2b+1)). Следовательно ≡0 (mod m).

**Пример 4:** Доказать что в каждой возрастающей арифметической прогрессии, состоящей из натуральных чисел, существует отрезок произвольной длины, состоящий только из составных чисел.

Рассмотрим арифметическую прогрессию b,b+a,b+2a,…, где a,bN, Пусть ,,..., - простые числа, причем a<<<...<. По Китайской теореме об остатках существует натуральное число, такое,что a≡-b-aj (mod ), где j=1,2,…,m. Это означает, что числа b+a(+1), b+a(+2), b+a(+m) являются составными.

**Пример 5:** Доказать что для любых натуральных чисел ,таких что )=)=…=(=1, уравнение   имеет бесконечно много натуральных решений. Если n=1,то , - решение уравнения = при любом z.Если n>2, то по китайской теореме об остатках существует бесконечно много таких чисел z, что z (mod ), z(mod ). Для каждого такого z числа

,…,,

являются решениями нашего уравнения.

**3. КТО. Применение к открытию сейфа в банке**

Бенджамен Франклин (Franklin) однажды сказал: «Трое могут хранить тайну, если двое из них мертвы». В этом параграфе мы изучаем безопасную систему допуска живых к секретным сведениям, основанную на китайской теореме об остатках. Представьте себе следующую ситуацию

Пусть -попарно взаимно простые числа, такие, что .Пусть S- произвольное целое число с условием M<S<N и - остатки от деления S на .

Предположим, далее, что в некотором банке работают n кассиров. Кассир с номером i знает пару чисел .Для открытия сейфа необходимо знать ключевое число S. Докажем, что любые k кассиров смогут открыть сейф, но никакие (k-1) кассиров не смогут это сделать. Действительно, пусть собрались кассиры с номерами , тогда им известен набор чисел По КТО можно найти такое число , что . Так как, то a=S (ввиду единственности решения этой системы сравнений по модулю) и ключевое число найдено, т.е. сейф можно открыть. Если собрались (k-1) кассиров, то они знают пары чисел. По КТО они могут найти такое целое число b, что и , т. е. b≠S. Таким образом, b не является искомым ключом к открытию сейфа.

В качестве конкретного примера можно рассмотреть числа : и,например, S=4001. Каждый из пяти кассиров знает одну из пар чисел (5,9), (1.10), (32,49), (32,53),(48,59).

Из предыдущего следует, что любые три кассира смогут найти ключ (равный S=4001) и открыть сейф, но никакие два не смогут этого сделать.

**Заключение**

В выше приведённой работе была сформулирована китайская теорема об остатках, приведены её доказательства, а также указанно применение КТО к решению олимпиадных задач и к некоторым прикладным вопросам теории чисел.

**Список литературы**

1. Бухштаб А.А. Теория чисел. - М: Просвящение,1996.

. Кузьмина А.С., Мальцев Ю.А. Теория чисел: учебное пособие/ А.С. Кузьмина, Ю.Н. Мальцев. - Барнаул: АлтГПА,2011.-240с.

. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. Москва: Постчаркет, 2001. - 328 с.

. Рыбников К.А. История математики: учебное пособие для университетов-Издательство Московского Университета,1960.