Министерство образования Российской Федерации

АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет математики и информатики

Н.В. Кван

ПРАКТИКУМ ПО ТЕОРИИ ЧИСЕЛ

ЧАСТЬ II

Учебно – методическое пособие

Благовещенск
2003

ББК
К

Печатается по решению
редакционно – издательского совета
факультета математики и информатики
Амурского государственного университета

Кван Н.В.

Практикум по теории чисел. Часть II. Учебно – методическое пособие. Благовещенск: Амурский гос. ун – т., 2003.

Настоящее пособие является продолжением методического пособия «Практикум по теории чисел. Часть I». Пособие разработано в помощь студентам 1 курса, изучающим теорию сравнений по курсу «Теория чисел» в соответствии с рабочей программой и содержанием государственного образовательного стандарта по специальности 010100. Пособие содержит теоретические сведения, решения типовых упражнений, задачи для самостоятельного решения, индивидуальные задания по темам «Решение сравнений с неизвестной величиной», «Арифметические приложения теории сравнений», вопросы к зачету.

Рецензент: Н.В. Ермак, доцент кафедры алгебры и геометрии БГПУ,
канд. физ.-мат. наук.

ВВЕДЕНИЕ

Теория чисел занимает важное место в системе математического образования будущих математиков. Данный курс тесно связан с основными математическими дисциплинами специальности «010100»: алгебра, линейная алгебра, дискретная математика, математическая логика, компьютерные науки.

Основной задачей теории чисел является изучение свойств целого числа. Ряд важных проблем этой теории непосредственно связан с понятием сравнения двух чисел по данному модулю. Изучению свойств сравнимых между собой чисел по данному модулю и арифметических приложений теории делимости посвящено данное учебно - методическое пособие.

Государственный образовательный стандарт высшего профессионального образования по теории чисел предусматривает изучение следующих тем (II часть): сравнения и их основные свойства; вычеты и классы вычетов по модулю m; кольцо классов вычетов; полная система вычетов; приведенная система вычетов; теорема Эйлера и Ферма; сравнения первой степени с одним неизвестным; теорема о существовании решений; простейшие приемы решений сравнений первой степени; системы сравнений; теоремы о решении системы сравнений первой степени; сравнения n-ой степени по простому модулю; теоремы о равносильности сравнений; теорема о числе решений; теорема Вильсона; сравнения n-ой степени по составному модулю; сравнения второй степени по простому модулю; квадратичные вычеты и невычеты; критерий Эйлера; символ Лежандра и его свойства; закон взаимности квадратичных вычетов; сравнения второй степени по составному модулю; первообразные корни и индексы; показатель числа по данному модулю; свойства показателей; первообразные корни по модулям p и $2p$; теорема об отыскании первообразных корней; индексы по модулям p и $2p$; таблица индексов; решение двучленных сравнений n-ой степени; показательные сравнения; арифметические приложения теории сравнений: отыскание остатков от деления некоторого числа на задуманное число; установление признаков делимости; понятие об алгебраических и трансцендентных числах.

Рабочая программа по курсу «Теория чисел», разработанная на основе государственного стандарта, предусматривает проведение 18 лекционных и 18 практических занятий со студентами – математиками I курса во втором семестре.

Данное учебно - методическое пособие содержит материал для проведения десяти практических занятий по теории сравнений Здесь приводятся необходимые теоретические сведения, подробные решения типовых примеров, задания для самостоятельного решения, а также два индивидуальных задания по темам практических занятий.

1. СРАВНЕНИЯ И ИХ СВОЙСТВА

Определение. Целые числа *a* и *b* называются сравнимыми по модулю *m*, если разность *a-b* делится на *m*.

Это соотношение записывают кратко так: $a \equiv b(\mathrm{mod}\, m)$.

Например, $17 \equiv 2 \ (\mathrm{mod}\ 5)$, $-7 \equiv 25\,(\mathrm{mod}\, 8)$.

Теорема. Число *a* сравнимо с *b* по модулю *m*, тогда и только тогда, когда *a* и *b* имеют одинаковые остатки при делении на *m* .

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

Из определений сравнимости следует, что число сравнимо по модулю со своим остатком при делении на модуль.

Сравнимые по данному модулю числа имеют с ним один и тот же НОД. Обратное утверждение неверно.

Все целые числа сравнимы между собой по модулю 1.

Свойства сравнений

1.Отношение сравнения есть отношение эквивалентности на множестве целых чисел **Z**:

а) отношение сравнения рефлексивно: $a \equiv a(\mathrm{mod}\, m)$;

б) отношение сравнения симметрично: если $a \equiv b(\mathrm{mod}\, m)$, то $\mathrm{b} \equiv \mathrm{a}(\mathrm{mod}\ \mathrm{m})$;

в)отношение сравнения транзитивно: если $a \equiv b(\mathrm{mod}\, m)$ и $\mathrm{b} \equiv \mathrm{c}(\mathrm{mod}\ \mathrm{m})$, то $\mathrm{a} \equiv \mathrm{c}\ (\mathrm{mod}\ \mathrm{m})$.

2. Если $a \equiv b(\mathrm{mod}\, m)$ и $\mathrm{c} \equiv \mathrm{d}\ (\mathrm{mod}\ \mathrm{m})$, то справедливо сравнение $a \pm c \equiv b \pm d\ (\mathrm{mod}\ m)$.

3. Если $a \equiv b(\mathrm{mod}\, m)$ и k - произвольное целое число, то $\mathrm{ka} \equiv \mathrm{kb}\ (\mathrm{mod}\ \mathrm{m})$.

4. Если $\mathrm{ka} \equiv \mathrm{kb}\ (\mathrm{mod}\ \mathrm{m})$ и $(\mathrm{k}, \mathrm{m}) = 1$, то $a \equiv b(\mathrm{mod}\, m)$.

5. Если $a \equiv b(\mathrm{mod}\, m)$ и k - произвольное натуральное число, то $\mathrm{ka} \equiv \mathrm{kb}\ (\mathrm{mod}\ \mathrm{k\ m})$.

6. Если $\mathrm{ka} \equiv \mathrm{kb}\ (\mathrm{mod}\ \mathrm{k\ m})$ и k - произвольное натуральное число, то $a \equiv b(\mathrm{mod}\, m)$.

7. Если $a \equiv b(\mathrm{mod}\, m)$ и $\mathrm{c} \equiv \mathrm{d}\ (\mathrm{mod}\ \mathrm{m})$, то справедливо сравнение $\mathrm{ac} \equiv \mathrm{bd}\ (\mathrm{mod}\ \mathrm{m})$.

8. Если $a \equiv b(\mathrm{mod}\, m)$, то при любом целом $n \geq 0$ $\mathrm{a}^{\mathrm{n}} \equiv \mathrm{b}^{\mathrm{n}}\ (\mathrm{mod}\ \mathrm{m})$.

9. Если $a \equiv b(\mathrm{mod}\, m)$ и $f(x) = c_0 + c_1 x + \mathrm{K} + c_n x^n$ - произвольный многочлен с целыми коэффициентами, то $f(a) \equiv f(b)\ (\mathrm{mod}\ \mathrm{m})$.

10.Если $a \equiv b(\mathrm{mod}\, m_1)$, $a \equiv b(\mathrm{mod}\, m_2)$, …, $a \equiv b(\mathrm{mod}\, m_n)$, то $a \equiv b(\mathrm{mod}\, m)$, где $m = [m_1, m_2, \mathrm{K}\ m_n]$.

11.В сравнении можно отбрасывать или добавлять слагаемые, делящиеся на модуль.

Пример 1. Найти остаток от деления на число 3 числа $A=13^{16}-2^{25}5^{15}$.

Решение. Очевидно, при делении на 3 число 13 равноостаточно с -1, а 5 тоже с -1. значит, число A при делении на 3 равноостаточно с числом

$$1^{16}\text{-}(-1)^{25}(-1)^{15}=1\text{-}1=0,$$

т.е. искомый остаток равен нулю, а число A делится на 3.

Пример 2. Найти остаток от деления числа 48^{5n+4} на 11 число, где n – любое целое неотрицательное число.

Решение. Известно, что к любой части сравнения можно прибавлять или отнимать числа, кратные модулю (это относится и к основанию степени). Используя это свойство сравнений, рассмотрим два случая:

а) $n=0$, тогда имеем:

$$48^4 \equiv 4^4 \equiv 16^2 \equiv 5^2 = 25 \equiv 4(\mathrm{mod}11),$$

б) $n\neq 0$, тогда последовательно имеем:

$$48^{5n+4}\equiv 4^{5n}4^4\equiv(4^5)^n\cdot 4\equiv(2^5)^{2n}4\equiv(-1)^{2n}4\equiv 4(\mathrm{mod}11).$$

Искомый остаток равен 4.

Пример 3. Доказать, что $2^{3^n}\equiv -1(\mathrm{mod}3^{n+1})$, где $n=1, 2, 3, \ldots$

Решение. При $n=1$ имеем верное сравнение $8\equiv -1(\mathrm{mod}3)$. Покажем, что, если для некоторого n исходное сравнение верно, то оно верно и для $n+1$.

Действительно, $2^{3^{n+1}}+1=(2^{3^n})^3+1=(2^{3^n}+1)(2^{2\cdot 3^n}-2^{3^n}+1)\equiv 0(\mathrm{mod}3^{n+2})$, так как $2^{3^n}+1\equiv 0(\mathrm{mod}3^{n+1})$ по допущению и $2^{2\cdot 3^n}-2^{3^n}+1\equiv 0(\mathrm{mod}3)$ в силу того, что $2\equiv -1(\mathrm{mod}3)$.

Пример 4. Показать, что сравнение $6^{89}\equiv 7(\mathrm{mod}16)$ не имеет места.

Решение. Известно, что, если $a\equiv b(\mathrm{mod}m)$, то $(a,m)=(b,m)$. В данном случае имеем:

$$(6^{89},16)=16,$$

но (7,16)=1, следовательно, сравнение $6^{89}\equiv 7(\mathrm{mod}16)$ не имеет места.

Пример 5. Доказать, что $(a+b)^p\equiv a^p+b^p(\mathrm{mod}\,p)$.

Решение. Рассмотрим разложение левой части сравнения по формуле бинома Ньютона $(a+b)^p=a^p+C_p^1a^{p-1}b+C_p^2a^{p-2}b^2+\mathrm{K}+C_p^{p-1}ab^{p-1}+b^p$, где $C_p^k=\dfrac{p!}{k!(p-k)!}$. Очевидно, что все биномиальные коэффициенты, кроме 1, кратны модулю p, а следовательно, сравнимы с 0 по модулю p.

УПРАЖНЕНИЯ

1. Какие из следующих сравнений являются верными: $3 \equiv 111 (\mathrm{mod}\, 49)$, $-7 \equiv 18 (\mathrm{mod}\, 5)$, $17 \equiv 239 (\mathrm{mod}\, 19)$, $(2n+1)^2 \equiv 0 (\mathrm{mod}\, 2)$?

2. Среди чисел 213, 458, 117, 185, 586, 132 найти все пары чисел, сравнимых между собой по модулю 7.

3. Даны три числа 137, 343, 633. какие из данных чисел сравнимы с 13 по модулю 31?

4. Записать в виде сравнений следующие утверждения:
а) число делится на 14; б) 17 – остаток от деления на 39 на 485; в) число N нечетно; г) число N имеет вид $3k+2$; д) число N имеет вид $12k-7$.

5. Найти все значения x, удовлетворяющие сравнениям:
а) $x \equiv 0 (\mathrm{mod}\, 3)$; б) $x \equiv 1 (\mathrm{mod}\, 2)$.

6 . Найти значения m, удовлетворяющие условию:
а) $21 \equiv 5 (\mathrm{mod}\, m)$; б) $3r+1 \equiv r+1 (\mathrm{mod}\, m)$.

7. Указать возможные значения модуля в сравнении $x \equiv 5 (\mathrm{mod}\, m)$, если известно, что этому сравнению удовлетворяет $x=13$.

8. Доказать, что следующие сравнения являются неверными:
а) $5^{1812} \equiv 1964 (\mathrm{mod} 125)$; б) $11^{207} \equiv 6 (\mathrm{mod} 21)$; в) $(2n+1)(2m+1) \equiv 2k (\mathrm{mod} 6)$, где n, m и k – числа целые.

9. Показать, что натуральное число, записанное в десятичной системе, сравнимо по модулю 9 и по модулю 3 с суммой своих цифр.

10. Найти остаток от деления на число 37 числа $A=13^{16} - 2^{25}5^{15}$.

11. Найти остаток от деления:
а) числа 48^{5n+3} на 11 число, где n – любое целое неотрицательное число;
б) числа 20^{6n+5} на 9 число, где n – любое целое неотрицательное число.

12. Показать, что при любом целом неотрицательном n число $3 \cdot 5^{2n+1} + 2^{3n+1}$ делится на 17.

13. При помощи сравнения ***Примера 3*** доказать, что существует бесконечное множество натуральных чисел $m>1$, удовлетворяет условию $2^m + 1 \equiv 0 (\mathrm{mod}\, m)$.

14. Доказать, что $(m-1)^{m^n} \equiv -1 (\mathrm{mod}\, m^{n+1})$, где $m>1$ – число нечетное и n – натуральное.

15. Доказать, что число вида $\frac{18a+5b}{19}$ есть целое, если известно, что число вида $\frac{11a+2b}{19}$ является целым (числа a и b – целые).

16. Пусть m и n - взаимно простые числа. Доказать, что если $a \equiv b (\mathrm{mod}\, m)$, $a \equiv b (\mathrm{mod}\, n)$, то $a \equiv b (\mathrm{mod}\, mn)$.

17. Доказать, что $(m-1)^{m^n} \equiv -1 (\mathrm{mod}\, m^{n+1})$, где $m>1$ – число нечетное и n- натуральное.

2. КЛАССЫ ВЫЧЕТОВ ПО ДАННОМУ МОДУЛЮ

Так как отношение сравнимости по модулю m обладает свойствами рефлексивности, симметричности и транзитивности, т.е. является отношением эквивалентности, оно индуцирует разбиение множества целых чисел $\boldsymbol{Z}$ на классы эквивалентности, которые называются классами вычетов по модулю m.

Множество всех классов вычетов по модулю m обозначается

$$\boldsymbol{Z/mZ}=\{0 \bmod m,\ 1 \bmod m,\ 2 \bmod m,\ \ldots,(m\text{-}1) \bmod m\}.$$

На этом множестве вводится операция +, определяемая равенством:

$$a \bmod m + b \bmod m = (a+b) \bmod m.$$

Алгебра $< \boldsymbol{Z/mZ, +} >$ является абелевой группой и называется аддитивной группой классов вычетов по модулю m.

На множестве классов вычетов по данному модулю вводится также операция умножения, определяемая равенством:

$$a \bmod m \cdot b \bmod m = (a \cdot b) \bmod m.$$

Алгебра $< \boldsymbol{Z/mZ, +,\cdot} >$ является коммутативным кольцом с единицей и называется кольцом классов вычетов по модулю m.

Кольцо классов вычетов по модулю m является полем тогда и только тогда, когда |m| - простое число.

Классы вычетов по модулю m, обладают следующими свойствами:

1. Любые два класса вычетов по модулю m либо совпадают. Либо не пересекаются. Объединение всех классов вычетов по модулю m совпадает с множеством всех целых чисел.

2. Пусть A и B – классы вычетов по модулю m, $a \in A$, $b \in B$. Классы A и B совпадают тогда и только тогда, когда $a \equiv b (\bmod m)$.

3. Если A – класс вычетов по модулю m и a – любой элемент из A, то $A=a+m\boldsymbol{Z}$,т.е. $A=\{a+mk/k \in \boldsymbol{Z}\}$.

Согласно свойству 1, каждый класс вычетов по модулю m однозначно определяется любым принадлежащим ему числом a; этот класс является множеством вида $\{a+mk/k \in \boldsymbol{Z}\}$. Класс вычетов по модулю m, содержащий число a, обозначается $\overline{a}$. Любое число, принадлежащее классу вычетов $\overline{a}$, называется представителем этого класса или вычетом.

Определение 1. Полной системой вычетов по некоторому модулю m называется система чисел, взятых по одному представителю из каждого класса по этому модулю.

Число вычетов в полной системе должно равняться числу классов, т. е. состоит из m чисел.

Среди полных систем вычетов по данному модулю выделяют: полную систему наименьших неотрицательных вычетов, т.е. совокупность чисел 0, 1, 2, …, m-1, полную систему наименьших положительных вычетов. т.е. совокупность чисел 1, 2, …,m, полную систему абсолютно наименьших вычетов, т.е.

совокупность чисел 0, ±1, ±2, …, $\pm\frac{m-1}{2}$ при нечетном m и $-\frac{m}{2}+1,...,-1,0,1,...,\frac{m}{2}$ при четном m.

Пример 1. Составить классы вычетов по модулю 8**.**

Решение. По модулю 8 имеется всего 8 классов вычетов:

$\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$, $\overline{6}$, $\overline{7}$ - полная система наименьших неотрицательных вычетов; $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$, $\overline{6}$, $\overline{7}$, $\overline{8}$ - полная система наименьших положительных вычетов; $\overline{0}$, $\pm\overline{1}$, $\pm\overline{2}$, $\pm\overline{3}$, $\overline{4}$ - полная система абсолютно наименьших вычетов.

Теорема 1. Любые m чисел: x_1, x_2, …, x_m попарно несравнимые между собой по модулю m, представляют собой полную систему вычетов.

Определение 2. Приведенной системой вычетов по данному модулю называется система чисел, взятых по одному из каждого класса, взаимно простого с модулем.

Теорема 2. Любые $\varphi(m)$ попарно несравнимых по модулю m и взаимно простых с этим модулем чисел представляют собой приведенную систему вычетов.

Пример 2. Составить приведенную систему вычетов по модулю 8**.**

Решение. Приведенная система вычетов по модулю 8 содержит $\varphi(8)=\varphi(2^3)=2^2(2-1)=4$ вычета. Рассмотрим полную систему наименьших положительных вычетов по модулю 8:

$$\overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5},\ \overline{6},\ \overline{7},\ \overline{8},$$

будем выбирать из этой системы только те вычеты, которые взаимно просты с модулем 8. Так как (1,8)=1, (2,8)=4, (3,8)=1, (4,8)=4, (5,8)=1, (6,8)=2, (7,8)=1, (8,8)=8, то приведенную систему вычетов по модулю 8 образуют классы вычетов $\overline{1}$, $\overline{3}$, $\overline{5}$, $\overline{7}$, не сравнимые между собой по модулю 8.

Произведение любых двух классов вычетов, взаимно простых с модулем m, тоже есть класс вычетов, взаимно простой с модулем m.

Множество классов вычетов по модулю m, взаимно простых с m, образует относительно умножения абелеву группу. Эта группа называется мультипликативной группой классов вычетов, взаимно простых с модулем.

УПРАЖНЕНИЯ

1. Найти полную систему наименьших неотрицательных вычетов, полную систему наименьших положительных вычетов и полную систему абсолютно наименьших вычетов по модулям 6, 19, 30.

2. Найти наименьшие положительные вычеты:

а) чисел по модулю 7; б) чисел по модулю 8; в) чисел по модулю 12.

3. Найти наименьшие неотрицательные вычеты:

а) чисел по модулю 5; б) чисел по модулю 10; в) чисел по модулю 16.

4. Найти абсолютно наименьшие вычеты:

а) чисел по модулю 9; б) чисел по модулю 11; в) чисел по модулю 24.

5. По какому модулю числа 34, -17, 12, -21, -50, 30 составляют полную систему вычетов?

6. Найти хотя бы одну полную систему вычетов вида $3x+1$ по модулю 9.

7. Образуют ли степени $2^0, 2^1, 2^2, \ldots, 2^{10}$ вместе с числом 0 полную систему вычетов по модулю 11?

8. Показать, что совокупность членов арифметической прогрессии *a, a+d, a+2d, a+3d, ..., a+(m-1)d* образует полную систему вычетов по модулю *m,* если *d* и *m* взаимно просты.

9. Написать несколько приведенных систем вычетов по модулю 12.

10. Доказать, что система чисел $5, 5^2, 5^3, 5^4, 5^5$ образует приведенную систему вычетов по модулю 7.

3. ТЕОРЕМА ЭЙЛЕРА И ФЕРМА

Теорема Эйлера. Если $(a,m)=1$, то $a^{\varphi(m)} \equiv 1(\mathrm{mod}\, m)$.

Доказательство. Пусть $r_1, r_2, \ldots, r_{\varphi(m)}$- некоторая приведенная система вычетов по модулю *m*. При $(a,m)=1$ числа $ar_1, ar_2, \ldots, ar_{\varphi(m)}$- также образуют приведенную систему вычетов по модулю *m*. Поставим в соответствие каждому из чисел $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ сравнимое с ним число из системы $r_1, r_2, \ldots, r_{\varphi(m)}$ так, что:

$$\begin{cases} ar_1 \equiv r_\alpha (\mathrm{mod}\, m) \\ ar_2 \equiv r_\beta (\mathrm{mod}\, m) \\ \ldots\ldots\ldots\ldots \\ ar_{\varphi(m)} \equiv r_\gamma (\mathrm{mod}\, m) \end{cases},$$

где $r_\alpha, r_\beta, \ldots, r_\gamma$ некоторым образом переставленные числа $r_1, r_2, \ldots, r_{\varphi(m)}$, т.е. $r_\alpha r_\beta \ldots r_\gamma = r_1 r_2 \ldots r_{\varphi(m)}$.

Перемножая все сравнения, получаем $a^{\varphi(m)} r_\alpha r_\beta \ldots r_\gamma \equiv r_1 r_2 \ldots r_{\varphi(m)} (\mathrm{mod} m)$.

Поскольку $(r_i, m)=1$ для всех I, то $(r_1 r_2 \ldots r_{\varphi(m)}, m)=1$ и обе части последнего сравнения можно сократить на $r_1 r_2 \ldots r_{\varphi(m)}$, так что $a^{\varphi(m)} \equiv 1(\mathrm{mod}\, m)$.

Теорема Ферма. Если $(a,p)=1$, то $a^{p-1} \equiv 1(\mathrm{mod}\, p)$.

Пример 1. Найти остаток от деления числа 5^{403} на 101.

Решение. 101 – простое число. Числа 5 и 101 взаимно простые, а поэтому из теоремы Ферма следует, что

$$5^{100} \equiv 1(\mathrm{mod}101).$$

Возведем это сравнение почленно в четвертую степень. Получим:

$$5^{400} \equiv 1(\mathrm{mod}101).$$

Кроме того, $5^3 \equiv 24(\mathrm{mod}101)$. Перемножим эти сравнения:

$$5^{403} \equiv 24(\mathrm{mod}101).$$

Из последнего сравнения вытекает, что искомый остатком будет число 24.

Пример 2. Найти последние две цифры числа 7^{325}.

Решение. Чтобы найти две последние цифры числа 7^{325}, нужно отыскать остаток от деления данного числа на число 100. Так как $(7,100)=1$, то по теореме Эйлера справедливо сравнение $7^{\varphi(100)} \equiv 1(\mathrm{mod}100)$, где $\varphi(100)=\varphi(2^2 5^2)=2^2 5^2(1-\frac{1}{2})(1-\frac{1}{5})=40$. Следовательно, $7^{40} \equiv 1(\mathrm{mod}100)$, $7^{320} \equiv 1(\mathrm{mod}100)$, $7^{320}7^5 \equiv 7^5(\mathrm{mod}100)$, $7^{325} \equiv 7^5(\mathrm{mod}100)$. Выясним, с каким числом сравнимо 7^5 по модулю 100. Очевидно сравнение $7^4 = 2401 \equiv 1(\mathrm{mod}100)$, а значит и сравнение $7^5 \equiv 7(\mathrm{mod}100)$.

Пример 3. Найти остаток от деления 126^{1020} на 138.

Решение. Здесь (126,138)=6. Если $x \equiv 126^{1020}(\mathrm{mod}138)$, то $x=6x_1$, $x_1 \equiv 21 \cdot 126^{1019} \equiv 21 \cdot 11^{22 \cdot 46+7} \equiv -2 \cdot 11^7 \equiv 11^6 \equiv 6^3 \equiv 9(\mathrm{mod}23)$, $x = 54 \equiv 2(\mathrm{mod}52)$. Остаток равен 2.

Пример 4. Показать, что число 37^{120} -1 делится на 700.

Решение. Простые числа 2, 5 и 7 взаимно просты с числом 37; следовательно, на основании теоремы Ферма справедливы сравнения: $37 \equiv 1(\mathrm{mod}2)$, $37^4 \equiv 1(\mathrm{mod}5)$, $37^6 \equiv 1(\mathrm{mod}7)$. Путем возведения обеих частей сравнений в соответствующие степени, получим сравнения: $37^{120} \equiv 1(\mathrm{mod}2)$, $37^{120} \equiv 1(\mathrm{mod}5)$, $37^{120} \equiv 1(\mathrm{mod}7)$. Воспользуемся свойством: если некоторое сравнение имеет место по нескольким модулям, то оно справедливо и по модулю, являющемуся наименьшим общим кратным данных модулей; поэтому, $37^{120} \equiv 1(\mathrm{mod}700)$, откуда $(37^{120}-1)\vdots 700$.

УПРАЖНЕНИЯ

1. Вычислить значения функции Эйлера $\varphi(13)$, $\varphi(125)$, $\varphi(360)$.
2. На основании свойств числовой функции Эйлера доказать, что в последовательности натуральных чисел существует бесконечное множество простых чисел.
3. Показать, что: а) число 13^{176}-1 делится на 89; b) 35^{40}-1 делится на 45.
4. Найти две последние цифры чисел: а) 517^{303}; б) 53^{323}; в) 36^{111}; г) 19^{2404}; д) $(116+17^{17})^{21}$.
5. Доказать, что: а) $(2^{32}+1)\vdots 641$; б) $(222^{555}+555^{222})\vdots 7$; в) $(220^{119^{69}}+69^{22^{119}}+119^{69^{220}})\vdots 102$.
6. Найти остаток от деления: а) 6^{592} на 11; б) $10^{40}+12^{40}$ на 25; в) $(12371^{56}+34)^{28}$ на 243.
7. Доказать, что $(3^{100}-3^{60}-3^{40}+1)\vdots 77$.
8. Доказать, что $a^{n(p-1)+1} \equiv a(\mathrm{mod}\,p)$.
9. Доказать, что при любом целом значении x: $x^{13} \equiv x(\mathrm{mod}2730)$.

10. Найти остаток от деления сотой степени целого числа на 125.

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

СРАВНЕНИЯ 1-ОЙ СТЕПЕНИ

Определение 1. Сравнение вида $f(x) \equiv 0 (\mathrm{mod}\, m)$, где

$f(x) = c_0 x^n + c_1 x^{n-1} + \mathrm{K} + c_{n-1} x + c_n$ - многочлен с целыми коэффициентами, называется сравнением с неизвестной величиной.

Теорема 1. Если некоторое число a удовлетворяет сравнению

$$f(x) \equiv 0 (\mathrm{mod}\, m),$$

то весь класс $\bar{a}$ состоит из чисел, удовлетворяющих этому сравнению.

Чтобы решить сравнение $f(x) \equiv 0 (\mathrm{mod}\, m)$, можно взять любую полную систему вычетов по модулю m: $x_1, x_2, \ldots, x_m$, вычислить $f(x_1), f(x_2), \ldots, f(x_m)$ и отобрать те x_i, при которых $f(x_i)$ делятся на m. Обычно в качестве полной системы вычетов берут систему абсолютно наименьших вычетов.

Определение 2. Два сравнения по одному и тому же модулю называются эквивалентными, если они имеют одни и те же решения

Определение 3. Сравнение вида $c_0 x + c_1 \equiv 0 (\mathrm{mod}\, m)$ называется сравнением первой степени с одним неизвестным.

Такое сравнение удобно записывать в виде $ax \equiv b (\mathrm{mod}\, m)$.

Теорема 2. Если $(a,m)=d$ и b не делится на d, то сравнение $ax \equiv b (\mathrm{mod}\, m)$ не имеет решений.

Теорема 3. Если $(a,m)=d$ и $b \vdots d$, то сравнение $ax \equiv b (\mathrm{mod}\, m)$ имеет d классов решений.

Теорема 4. Если $(a,m)=1$ b, то сравнение $ax \equiv b (\mathrm{mod}\, m)$ имеет единственное решение.

Методы решений сравнений

1. Метод испытания вычетов.

Пример 1. Решить сравнение $4x \equiv 3 (\mathrm{mod}\, 7)$.

Решение. Данное сравнение имеет единственное решение, т.к. (4,7)=1. Подвергнем испытанию вычеты по модулю 7: 0, 1, 2, 3, 4, 5, 6.

При $x=0$, $0 \equiv 3 (\mathrm{mod}\, 7)$ - неверное сравнение; при $x=1$, $4 \equiv 3 (\mathrm{mod}\, 7)$ - неверное сравнение; при $x=2$, $8 \equiv 3 (\mathrm{mod}\, 7)$ - неверное сравнение; при $x=3$, $24 \equiv 3 (\mathrm{mod}\, 7)$ - верное сравнение. Таким образом, решением данного сравнения является класс вычетов, сравнимых с 3 по модулю 7, т.е. $x \equiv 3 (\mathrm{mod}\, 7)$.

2. Метод с использованием теоремы Эйлера.

Сравнение $ax \equiv b (\mathrm{mod}\, m)$, где $(a,m)=1$, имеет решение в виде

$$x \equiv a^{\varphi(m)-1} b (\mathrm{mod}\, m).$$

Пример 2. Решить сравнение $5x \equiv 6 (\mathrm{mod}\, 7)$.

Решение. Так как (5,7)=1, сравнение имеет единственное решение, представимое в виде $x \equiv 5^{\varphi(7)-1}6(\mathrm{mod}\,7)$. Значение $\varphi(7)$ равно 6, а следовательно $x \equiv 5^5 6(\mathrm{mod}\,7)$. Заменим число $5^5 6$ наименьшим неотрицательным вычетом по модулю 7: $x \equiv 4(\mathrm{mod}\,7)$.

3. Метод с использованием конечных дробей.

Сравнение $ax \equiv b(\mathrm{mod}\,m)$, где $(a,m)=1$, имеет решение в виде

$$x \equiv (-1)^s P_{s-1} b(\mathrm{mod}\,m),$$

где P_{s-1} – числитель предпоследней подходящей дроби конечной цепной дроби, соответствующей $\frac{m}{a}$.

Пример 3. Решить сравнение $113x \equiv 89(\mathrm{mod}\,312)$.

Решение. Так как (113,312)=1, сравнение имеет единственное решение.

Найдем разложение дроби $\frac{312}{113}$ в конечную цепную дробь:

$$312=113\cdot 2+86,$$
$$113=86\cdot 1+27,$$
$$86=27\cdot 3+5,$$
$$27=5\cdot 5+2,$$
$$5=2\cdot 2+1,$$
$$2=1\cdot 2;$$

т.е. $\frac{312}{113}=[2;\ 1,\ 3,\ 5,\ 2,\ 2]$.

Составим таблицу для нахождения числителя предпоследней подходящей дроби

k		0	1	2	3	4	5=s
q_k		2	1	3	5	2	2
P_k	1	2	3	11	58	127=P_{s-1}	312

Таким образом, решение сравнения будет иметь вид:

$$x \equiv (-1)^5 \cdot 127 \cdot 89(\mathrm{mod}\,312),\ x \equiv -11303(\mathrm{mod}\,312),\ x \equiv 241(\mathrm{mod}\,312).$$

4. Метод с использованием свойств сравнений.

Если $(a,m)=1$, то сравнение $ax \equiv b(\mathrm{mod}\,m)$ можно заменить эквивалентными сравнениями: $ax \equiv b \pm m(\mathrm{mod}\,m)$, $ax \equiv b \pm 2m(\mathrm{mod}\,m)$, $ax \equiv b \pm 3m(\mathrm{mod}\,m)$, … , пока не попадется сравнение, в котором левую и правую части можно сократить на a.

Причем число испытываемых сравнений будет не больше, чем a.

Этот способ целесообразен при небольших значениях a.

Пример 4. Решить сравнение $5x \equiv 3(\mathrm{mod}\,11)$.

Решение. Данное сравнение имеет единственное решение, которое можно найти, прибавив к правой части сравнения $2m$: $5x \equiv 3+2\cdot 11(\mathrm{mod}\,11)$, $5x \equiv 25(\mathrm{mod}\,11)$, $x \equiv 5(\mathrm{mod}\,11)$.

Пример 5. Решить сравнение $10x \equiv 25(\mathrm{mod}\,35)$.

Решение. Данное сравнение имеет 5 классов решений, т.к. (10,35)=5 и 25№5. разделим обе части сравнения и модуль на 5. Получим сравнение по новому модулю m_1=7: $2x \equiv 5(\mathrm{mod}\,7)$. Решим полученное сравнение, прибавив к его правой части один модуль, т.е. $2x \equiv 12(\mathrm{mod}\,7)$, $x_0 \equiv 6(\mathrm{mod}\,7)$ или $x = 6 + m_1 t, \quad t \in Z$. Решения начального сравнения найдем по формуле: $x = 6 + m_1 t, \quad t = 0,1,2,3,4.$

$$x_1 = 6 + 7 \cdot 0, \quad x \equiv 6(\mathrm{mod}\,35);$$
$$x_2 = 6 + 7 \cdot 1, \quad x \equiv 13(\mathrm{mod}\,35);$$
$$x_3 = 6 + 7 \cdot 2, \quad x \equiv 20(\mathrm{mod}\,35);$$
$$x_4 = 6 + 7 \cdot 3, \quad x \equiv 27(\mathrm{mod}\,35);$$
$$x_5 = 6 + 7 \cdot 4, \quad x \equiv 34(\mathrm{mod}\,35).$$

Пример 6. Решить сравнение $12x \equiv 9(\mathrm{mod}\,18)$.

Решение. Замечаем, что (12,18)=6. Но при этом число 9 не делится нацело на 6. Поэтому данное сравнение не имеет решений.

Пример 7. Решить сравнение $(m+1)^2 x \equiv a(\mathrm{mod}\,m)$.

Решение. Воспользуемся формулой квадрата суммы и запишем сравнение в виде $(m^2 + 2m + 1)x \equiv a(\mathrm{mod}\,m)$. Видим, что первые два слагаемых делятся на m; следовательно $x \equiv a(\mathrm{mod}\,m)$.

УПРАЖНЕНИЯ

1. Решить сравнения:
   a) $3x \equiv 8(\mathrm{mod}\,12)$,
   b) $17x \equiv 89(\mathrm{mod}\,4)$,
   c) $6x \equiv 2(\mathrm{mod}\,9)$,
   d) $21x \equiv 5(\mathrm{mod}\,35)$,
   e) $5x \equiv 1(\mathrm{mod}\,11)$,
   f) $2x \equiv 7(\mathrm{mod}\,15)$,
   g) $7x \equiv 10(\mathrm{mod}\,13)$,
   h) $97x \equiv 11(\mathrm{mod}\,41)$,
   i) $81x \equiv 14(\mathrm{mod}\,202)$,
   j) $23x \equiv 175(\mathrm{mod}\,71)$,
   k) $505x \equiv 85(\mathrm{mod}\,565)$,
   l) $60x \equiv 44(\mathrm{mod}\,164)$,
   m) $243x \equiv 271(\mathrm{mod}\,317)$,
   n) $486x \equiv 542(\mathrm{mod}\,634)$,
   o) $84x \equiv 34(\mathrm{mod}\,156)$,
   p) $111x \equiv 75(\mathrm{mod}\,321)$.
2. Решить сравнения при условии $(a,b)=1$:
   a) $(a+b)x \equiv a^2 + b^2(\mathrm{mod}\,ab)$;
   b) $(a^2 + b^2)x \equiv a - b \ (\mathrm{mod}\,ab)$;
   c) $(a+b)^2 x \equiv a^2 - b^2(\mathrm{mod}\,ab)$.
3. Решить сравнения:

a) $ax \equiv 1 (\mathrm{mod}\, p)$, $(a, p) = 1$;

b) $(a+1)x \equiv a^2 - 1 (\mathrm{mod}\, m)$.

4. НЕОПРЕДЕЛЕННЫЕ УРАВНЕНИЯ 1 СТЕПЕНИ

Теоремы о числе решений сравнений 1-ой степени можно применить к решению неопределенных (диофантовых) уравнений 1-ой степени.

Рассмотрим уравнение $ax+by=c$, где $(a,b)=d$, $a\neq 0$, $b\neq 0$ и c . Перепишем это уравнение в виде $ax=c-by$, а затем в виде сравнения $ax \equiv c (\mathrm{mod}\, b)$. Решим это сравнение, разделив обе его части и модуль на d. Получим класс чисел $x = x_0 + bt$, $t \in \boldsymbol{Z}$, удовлетворяющих данному диофантову уравнению, где x_0 - решение сравнения $\frac{a}{d}x \equiv \frac{c}{d} (\mathrm{mod} \frac{b}{d})$. Для нахождения соответствующих значений y запишем неопределенное уравнение в виде $a(x_0 + bt) + by = c$. Отсюда $y = \frac{c - ax_0}{b} - at$, $t \in \boldsymbol{Z}$ или $y = y_0 - at$. Итак, обще решение диофантова уравнения имеет вид:

$$\begin{cases} x = x_0 + bt, \\ y = y_0 - at, \end{cases} t \in \boldsymbol{Z}.$$

Пример 1. Решить уравнение $26x - 44y = 38$.

Решение. Здесь (26,44)=2 и 38 2. Решим сравнение $26x \equiv 38 (\mathrm{mod}\, 44)$. Для этого разделим обе части сравнения и модуль на их НОД, равный 2. Получим сравнение $13x \equiv 19 (\mathrm{mod}\, 22)$, имеющее решение $x \equiv 15 (\mathrm{mod}\, 22)$. Тогда $x_0 \equiv 15$ и $13 \cdot 15 - 22y_0 = 19$, $y_0 = 8$.

Следовательно, любое решение данного диофантова уравнения имеет вид:

$x = 15 + 22t$, $y = 8 + 13t$, где t – любое целое число.

Пример 2. Разложить дробь $\frac{19}{21}$ на сумму или разность двух дробей соответственно со знаменателями 3 и 7.

Решение. Из условия получаем $\frac{x}{3} + \frac{y}{7} = \frac{19}{21}$, откуда $7x+3y=19$; т.к. (3,7)=1, то уравнение имеет решение в целых числах. Приходим к сравнению

$$7x \equiv 19 (\mathrm{mod}\, 3)$$

и последовательно имеем:

$$4x \equiv 1 (\mathrm{mod}\, 3),$$

$$x \equiv 1 (\mathrm{mod}\, 3),$$

$$x = 1 + 3t \text{ и } y = \frac{19 - 7 \cdot 1}{3} - 7t = 4 - 7t.$$

Достаточно положить t=0. Получим x=1, y=4 и окончательно $\frac{1}{3}+\frac{4}{7}=\frac{19}{21}$.

Пример 3. Какое наименьшее натуральное число надо умножить на 7, чтобы произведение оканчивалось на 123?

Решение. Заметим, что числа 7 и 10 взаимно просты, а число123 состоит из трех цифр; тогда уравнение $7x-10^n y=1$ имеет целые положительные решения, где n=3. Умножив левую и правую части уравнения на число 123, получим искомое число $x\cdot 123$, где x- корень уравнения $7x-1000y=1$.

Решим уравнение $7x-1000y=1$:

$$7x\equiv 1(\mathrm{mod}1000),$$
$$x\equiv 143(\mathrm{mod}1000),$$

тогда $143\cdot 123=123123$ – искомое число.

УПРАЖНЕНИЯ

1. Решить уравнения:

a) $7x-72y=5$,
b) $37x+107y=25$,
c) $41x-7y=28$,
d) $505x-85y=565$,
e) $52x+23y=1$,
f) $4997x+4009y=3$,
g) $1414x+406y=42$,
h) $2977x-1469y=13$.

2. Разложить дробь на сумму или разность двух дробей с соответствующими знаменателями:

a) дробь - $\frac{13}{15}$, знаменатели 3 и 5;
b) дробь - $\frac{37}{55}$, знаменатели 5 и 11;
c) дробь - $\frac{68}{143}$, знаменатели 11 и 13.

3. Для перевозки зерна имеются мешки по 60 *кг* и по 80 *кг*. Сколько нужно тех и других мешков для перевозки 440 *кг* зерна?

4. Какие две цифры следует приписать к числу 32, чтобы полученное четырехзначное число делилось на 3 и на 7?

5. При каких наименьших натуральных значениях a и b уравнение $ax-by=31$ имеет решение x=5, y=9?

6. На прямой $8x-13y+6=0$ найти число целых точек, лежащих между прямыми x=-110 и x=150.

7. Доказать, что внутри прямоугольника, ограниченного прямыми x=-2, x=5 и y=-1, y=2, на прямой $3x-7y=1$ не лежит ни одной целой точки.

8. Найти год рождения тех людей, которым в 2002 году исполнилось столько лет какова сумма цифр года их рождения.

9. Найти все четырехзначные простые числа, начинающиеся и оканчивающиеся цифрой 1.

10. Найти четырехзначные числа, которые, будучи приписаны справа к числу 400, дают полный квадрат.

5. СИСТЕМЫ СРАВНЕНИЙ 1-ОЙ СТЕПЕНИ

Рассмотрим систему сравнений 1-й степени с одним неизвестным

$$\begin{cases} x \equiv c_1 \pmod{m_1}, \\ x \equiv c_2 \pmod{m_2}. \end{cases}$$

Теорема 1. Пусть d – наибольший общий делитель, M - наименьшее общее кратное m_1 и m_2 тогда если разность $c_2 - c_1$ не делится нацело на d, то система не имеет решений, а если $(c_2 - c_1) \vdots d$, то система имеет единственное решение, представляющее класс по модулю M.

Если m_1 и m_2 взаимно просты, то $d=1$, $M= m_1 m_2$. А следовательно для таких модулей система всегда имеет одно решение, представляющее собой класс по модулю $m_1 m_2$.

Пример 1. Исследовать системы сравнений

$$\text{а)} \begin{cases} x \equiv 3 \pmod 7, \\ x \equiv 6 \pmod{12} \end{cases} \quad \text{б)} \begin{cases} x \equiv 4 \pmod{35}, \\ x \equiv 8 \pmod{15} \end{cases}$$

и решить их в случае совместности.

Решение. а) Поскольку (7,12)=1, система имеет решение. Из первого сравнения системы запишем x в виде $x=9+7t$, подставим данное выражение во вторую систему и найдем t , решив вторую систему:

$$9 + 7t \equiv 6 \pmod{12}, \; 7t \equiv -3 \pmod{12}, \; 7t \equiv -3 + 24 \pmod{12}, \; t \equiv 3 \pmod{12},$$

$$t = 3 + 12y.$$

Подставляя это значение t в выражение для x, имеем:

$$x=9+7(3+12y)=30+84y; \; x \equiv 30 \pmod{84}.$$

б) Поскольку (15,35)=5 и разность чисел 8 и 4 не делится на 5, то система не имеет решение.

Пример 2. Исследовать систему сравнений

$$\begin{cases} 7x \equiv 10 \pmod{13}, \\ 2x \equiv 2 \pmod 6 \end{cases}$$

и решить ее в случае совместности.

Решение. Так как (13,6)=1, система имеет решение. Заметим, что второе сравнение системы имеет два решения, потому что обе части сравнения и модуль имеют НОД равный 2. Следовательно, данная система распадается на две системы сравнений:

$$\begin{cases} 7x \equiv 10 \pmod{13}, \\ x \equiv 1 \pmod 6 \end{cases} \text{ и } \begin{cases} 7x \equiv 10 \pmod{13}, \\ x \equiv 4 \pmod 6. \end{cases}$$

Решим первую систему. Для этого запишем x в виде $x=1+6t$, подставим данное выражение в первое сравнение и найдем t :

$$7 + 42t \equiv 10 \pmod{13}, \; 3t \equiv 3 \pmod{13}, \; t \equiv 1 \pmod{13}, \; t = 1 + 13y.$$

Подставляя это значение t в выражение для x, имеем:

$$x=1+6(1+13y)=7+78y; \; x \equiv 7 \pmod{78}.$$

Решим вторую систему:

$$x=4+6t,\ 28+42t\equiv 10(\mathrm{mod}13),\ 3t\equiv -18(\mathrm{mod}13),$$

$$t\equiv -6(\mathrm{mod}13),\ t\equiv 7(\mathrm{mod}13),\ t=7+13y,\ x=4+6(7+13y)=46+78y;\ x\equiv 46(\mathrm{mod}78).$$

Таким образом, данная система сравнений имеет два решения:

$$x\equiv 7(\mathrm{mod}78)\ \text{ и }\ x\equiv 46(\mathrm{mod}78).$$

Дана система сравнений:

$$\begin{cases} a_1 x\equiv b_1(\mathrm{mod}\,m_1), \\ a_2 x\equiv b_2(\mathrm{mod}\,m_2), \end{cases}$$

где $(m_1,m_2)=(a_1,m_1)=(a_2,m_2)=1$. Эту систему сравнений можно заменить эквивалентной ей системой:

$$\begin{cases} x\equiv c_1(\mathrm{mod}\,m_1), \\ x\equiv c_2(\mathrm{mod}\,m_2), \end{cases}$$

где первое и второе из сравнений этой системы является соответственно решениями исходной системы сравнений.

От полученной системы перейдем к системе

$$\begin{cases} m_2 x\equiv c_1(\mathrm{mod}\,m_1\cdot m_2), \\ m_1 x\equiv c_2(\mathrm{mod}\,m_1\cdot m_2), \end{cases}$$

эквивалентной данной и имеющей единственное решение по модулю $m_1\cdot m_2$.

При решении системы сравнений рассмотренным способом в случае попарно взаимно простых модулей нет необходимости заменять исходную систему системой $\begin{cases} x\equiv c_1(\mathrm{mod}\,m_1), \\ x\equiv c_2(\mathrm{mod}\,m_2). \end{cases}$

Пример 3. Решить систему сравнений:

$$\begin{cases} 5x\equiv 7(\mathrm{mod}11), \\ 2x\equiv 3(\mathrm{mod}5). \end{cases}$$

Решение. Так как $(5,11)=(5,11)=(2,5)=1$, то каждое сравнение системы имеет единственное решение, а сама система имеет единственное решение по модулю 55.

От данной системы переходим к системе сравнений

$$\begin{cases} 25x\equiv 35(\mathrm{mod}55), \\ 22x\equiv 33(\mathrm{mod}55) \end{cases}$$

и, вычитая из первого второе сравнение, получаем сравнение $3x\equiv 2(\mathrm{mod}55)$, решение которого $x\equiv 19(\mathrm{mod}55)$ является решением исходной системы.

Теорема 2. Система сравнений

$$\begin{cases} x\equiv c_1(\mathrm{mod}\,m_1), \\ x\equiv c_2(\mathrm{mod}\,m_2), \\ \quad\cdots\cdots\cdots\cdots \\ x\equiv c_n(\mathrm{mod}\,m_n) \end{cases}$$

Либо совсем не имеет решений, либо имеет решение, представляющее собой класс по модулю, равному наименьшему кратному чисел:

$$m_1, m_2, \ldots, m_n.$$

Найти решение подобной системы можно, решив сначала первые два сравнения, добавив потом последовательно третье и т. д., пока не будет исчерпана вся система.

Пример 4. Решить систему сравнений:

$$\begin{cases} x \equiv 1 (\mathrm{mod}\, 2), \\ x \equiv 3 (\mathrm{mod}\, 7), \\ x \equiv 5 (\mathrm{mod}\, 10). \end{cases}$$

Решение. Решаем сначала систему, состоящую из двух первых сравнений:

$$x=1+2t \equiv 3(\mathrm{mod}\, 7),\ 2t \equiv 2(\mathrm{mod}\, 7),\ t \equiv 1(\mathrm{mod}\, 7),\ t = 1 + 7y,$$

$$x=1+2(1+7y)=3+14y;\ x \equiv 3(\mathrm{mod}\, 14).$$

Таким образом, данная система эквивалентна системе:

$$\begin{cases} x \equiv 3(\mathrm{mod}\, 14), \\ x \equiv 5(\mathrm{mod}\, 10). \end{cases}$$

Здесь (10,14)=2 и $2 \mid 14-10$, так что система совместна. Решаем ее:

$$x=3+14t \equiv 5(\mathrm{mod}\, 10),\ 14t \equiv 2(\mathrm{mod}\, 10),\ 7t \equiv 1(\mathrm{mod}\, 5),\ 7t \equiv 21(\mathrm{mod}\, 5),\ t \equiv 3(\mathrm{mod}\, 5),$$

$$t = 3 + 5y,\ x=3+14(3+5y)=45+70y;\ x \equiv 45(\mathrm{mod}\, 70).$$

Теорема 3 (китайская теорема об остатках). Пусть $m_1, m_2, \ldots, m_n$ – попарно взаимно простые числа, $M=m_1 \cdot m_2, \cdot \ldots \cdot m_n$; $y_1, y_2, \ldots, y_n$ подобраны так, что

$$\frac{M}{m_1} y_1 \equiv 1(\mathrm{mod}\, m_1),\ \frac{M}{m_2} y_2 \equiv 1(\mathrm{mod}\, m_2),\ \ldots,\ \frac{M}{m_n} y_n \equiv 1(\mathrm{mod}\, m_n),$$

$$x_0=\frac{M}{m_1} y_1 c_1 + \frac{M}{m_2} y_2 c_2 + \ldots + \frac{M}{m_n} y_n c_n.$$

Тогда решение системы:

$$\begin{cases} x \equiv c_1 (\mathrm{mod}\, m_1), \\ x \equiv c_2 (\mathrm{mod}\, m_2), \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv c_n (\mathrm{mod}\, m_n) \end{cases}$$

будет иметь вид $x \equiv x_0 (\mathrm{mod}\, M)$.

Пример 5. Решить систему сравнений:

$$\begin{cases} x \equiv 7(\mathrm{mod}\, 11), \\ x \equiv -5(\mathrm{mod}\, 13), \\ x \equiv 8(\mathrm{mod}\, 14). \end{cases}$$

Решение. Находим:

$$13\cdot 14y_1 \equiv 1(\mathrm{mod}\,11),\quad 6y_1 \equiv 1(\mathrm{mod}\,11),\qquad y_1 = 2;$$
$$11\cdot 14y_2 \equiv 1(\mathrm{mod}\,13),\quad 11y_2 \equiv 1(\mathrm{mod}\,13),\qquad y_2 = 11;$$
$$11\cdot 13y_3 \equiv 1(\mathrm{mod}\,14),\quad 3y_3 \equiv 1(\mathrm{mod}\,14),\qquad y_3 = 5;$$
$$x = 13\cdot 14\cdot 2\cdot 7 - 11\cdot 14\cdot 11\cdot 5 + 11\cdot 13\cdot 5\cdot 8 \equiv -202(\mathrm{mod}\,11\cdot 13\cdot 14);$$
$$x \equiv 1800(\mathrm{mod}\,2002).$$

Пример 6. Найти значение параметра a, при которых имеет решение система сравнений $\begin{cases} 2x \equiv a(\mathrm{mod}\,4), \\ 3x \equiv 4(\mathrm{mod}\,10). \end{cases}$

Решение. Решим второе сравнение системы: $\begin{cases} 2x \equiv a(\mathrm{mod}\,4), \\ x \equiv 8(\mathrm{mod}\,10). \end{cases}$ Первое сравнение имеет решение тогда и только тогда, когда $a \equiv 0(\mathrm{mod}\,2)$ или $a = 2q$. При этих значениях a данная система равносильна следующей: $\begin{cases} x \equiv q(\mathrm{mod}\,2), \\ x \equiv 8(\mathrm{mod}\,10). \end{cases}$ данная система сравнений имеет решение лишь при $q \equiv 0(\mathrm{mod}\,2)$ или $q = 2q_1$, откуда $a = 4q_1$ или $a \equiv 0(\mathrm{mod}\,4)$.

УПРАЖНЕНИЯ

1. Решить системы сравнений:

a) $\begin{cases} x \equiv 3(\mathrm{mod}\,7), \\ x \equiv 5(\mathrm{mod}\,9); \end{cases}$

b) $\begin{cases} x \equiv 6(\mathrm{mod}\,9), \\ x \equiv 9(\mathrm{mod}\,12); \end{cases}$

c) $\begin{cases} 7x \equiv 10(\mathrm{mod}\,11), \\ 5x \equiv 3(\mathrm{mod}\,6); \end{cases}$

d) $\begin{cases} x \equiv 2(\mathrm{mod}\,8), \\ 3x \equiv 6(\mathrm{mod}\,9); \end{cases}$

e) $\begin{cases} 28x \equiv 40(\mathrm{mod}\,44), \\ 2x \equiv 3(\mathrm{mod}\,5); \end{cases}$

f) $\begin{cases} x \equiv 7(\mathrm{mod}\,13), \\ x \equiv 5(\mathrm{mod}\,10), \\ x \equiv 2(\mathrm{mod}\,3); \end{cases}$

g) $\begin{cases} x \equiv 4(\mathrm{mod}\,15), \\ x \equiv 1(\mathrm{mod}\,12), \\ x \equiv 7(\mathrm{mod}\,14); \end{cases}$

h) $\begin{cases} 9x \equiv 12(\mathrm{mod}\,21), \\ 9x \equiv 2(\mathrm{mod}\,14), \\ 2x \equiv 1(\mathrm{mod}\,11); \end{cases}$

k) $\begin{cases} 2x \equiv 6(\mathrm{mod}\,12), \\ 3x \equiv 5(\mathrm{mod}\,14), \\ 12x \equiv 7(\mathrm{mod}\,13); \end{cases}$

l) $\begin{cases} 5x \equiv 200(\mathrm{mod}\,251), \\ 11x \equiv 192(\mathrm{mod}\,401), \\ 3x \equiv -1512(\mathrm{mod}\,9073); \end{cases}$

$$\text{m)}\begin{cases} x \equiv 1(\mathrm{mod}\,25), \\ x \equiv 2(\mathrm{mod}\,4), \\ x \equiv 3(\mathrm{mod}\,7), \\ x \equiv 4(\mathrm{mod}\,9). \end{cases}$$

2. При каких значениях параметра a следующие системы сравнений совместны:

$$\text{a)}\begin{cases} x \equiv 5(\mathrm{mod}\,18), \\ x \equiv 8(\mathrm{mod}\,21), \\ x \equiv a(\mathrm{mod}\,35); \end{cases}$$

$$\text{b)}\begin{cases} x \equiv 3(\mathrm{mod}\,11), \\ x \equiv 11(\mathrm{mod}\,20), \\ x \equiv 1(\mathrm{mod}\,15), \\ x \equiv a(\mathrm{mod}\,18). \end{cases}$$

6. СРАВНЕНИЯ ПО ПРОСТОМУ МОДУЛЮ

Будем рассматривать сравнения n-ой степени по простому модулю p:

$$c_0 x^n + c_1 x^{n-1} + \mathrm{K} + c_{n-1} x + c_n \equiv 0 (\mathrm{mod}\, p). \qquad (1)$$

Теорема 1. Если c_0 не делится нацело на p, то сравнение (1) может быть заменено эквивалентным сравнением с коэффициентом при старшем члене, равном 1.

Пример 1. Сравнение

$$6x^5-3x^3+4x^2-x+3\equiv 0(\mathrm{mod}\ 13)$$

заменить равносильным ему сравнением со старшим коэффициентом, равным 1.

Решение. Так как старший коэффициент данного сравнения равен 6 и (6,13)=1, то сравнение $6y\equiv 1(\mathrm{mod}\ 13)$ имеет единственное решение

$$y\equiv 11(\mathrm{mod}\ 13).$$

Умножим сравнение

$$6x^5-3x^3+4x^2-x+3\equiv 0(\mathrm{mod}\ 13)$$

на число 11, не меняя модуля сравнения:

$$66x^5-33x^3+44x^2-11x+33\equiv 0(\mathrm{mod}\ 13).$$

Заменяя каждый коэффициент сравнения на наименьший вычет по модулю 13, получаем сравнение

$$x^5+6x^3+5x^2+2x+6\equiv 0(\mathrm{mod}\ 13)$$

эквивалентное данному.

Теорема 2.Если $f(x)$ и $g(x)$ многочлены с целыми коэффициентами, то сравнения $f(x)\equiv 0(\mathrm{mod}\ p)$ и $f(x)-(x^p-x)g(x)\equiv 0(\mathrm{mod}\ p)$ по простому модулю p эквивалентны.

Теорема 3. Сравнение по простому модулю p, степень которого больше или равна, чем этот модуль, может быть заменено эквивалентным сравнением степени, меньшей чем p.

Пример 2. Заменить сравнение

$$x^{14}-4x^{13}-x+6\equiv 0(\text{mod } 7).$$

равносильным ему сравнением, степень которого ниже p, где p – модуль.

Решение. Разделим многочлен, стоящий в левой части сравнения на многочлен x^7-x с остатком, согласно известному способу деления многочлена на многочлен:

$$x^{14}-4x^{13}-x+6=(x^7-x)(x^7-4x^6+x-4)+x^2-5x-6.$$

Степень остатка

$$r(x)= x^2-5x-6$$

меньше степени x^7-x, и так как

$$r(x)= f(x) -(x^p-x)g(x),$$

то по ***Теореме 2*** сравнения $f(x) \equiv 0(\text{mod } p)$ и $r(x)\equiv 0(\text{mod } p)$ эквивалентны.

Следовательно, сравнение равносильное данному, степень которого ниже семи, имеет вид:

$$x^2-5x-6\equiv 0(\text{mod } 7).$$

Практически удобней заменять каждое слагаемое многочлена x^s, где $s \geq p$, слагаемым

$$x^s -(x^s -x)x^{s-p}=x^{s-(p-1)}$$

степени, меньшей, чем s.

Пример 3. Разложить многочлен

$$x^4+x+4$$

на множители по модулю 11.

Решение. Рассмотрим сравнение

$$x^4+x+4\equiv 0(\text{mod } 11).$$

При помощи испытания вычетов выясним, что данное сравнение имеет решение

$$x\equiv 2(\text{mod } 11),$$

а поэтому справедливо сравнение

$$x^4+x+4\equiv (x-2)(x^3+2x^2+4x+9)(\text{mod } 11).$$

Рассмотрим далее сравнение

$$x^3+2x^2+4x+9\equiv 0(\text{mod } 11).$$

И аналогично, испытанием вычетов найдем его решение

$$x\equiv 3(\text{mod } 11),$$

а поэтому

$$x^4+x+4\equiv (x-2)(x-3)(x^2+5x+8)(\text{mod } 11)$$

или

$$x^4+x+4\equiv (x-2)(x-3)(x^2-6x+8)(\text{mod } 11),$$

что равносильно

$$x^4+x+4\equiv (x-2)^2(x-3)(x-4)(\text{mod } 11).$$

Следовательно, искомое разложение имеет вид

$$x^4+x+4=(x-2)^2(x-3)(x-4)(\text{mod } 11).$$

Теорема 4. Сравнение степени n по простому модулю p с коэффициентом при старшем члене, не делящемся на p, может иметь не более n решений.

Для составных модулей эта теорема неверна.

Теорема 5. Если сравнение степени n по простому модулю p $f(x)\equiv 0(\mathrm{mod}\ p)$ имеет n решений тогда и только тогда, когда коэффициенты остатка от деления $x^{p-1}-1$ на $f(x)$ кратны p.

Пример 3. Имеет ли сравнение $x^2-2x+2\equiv 0(\mathrm{mod}\ 5)$ максимальное число решений?

Решение. Данное сравнение может иметь не более двух решений. Наибольшее число решений оно будет иметь, если при делении многочлена x^5-x на левую часть сравнения получим остаток, коэффициенты которого кратны модулю. Имеем,

$$x^5-x=(x^2-2x+2)(x^3+2x^2+2x)-5x\ ;$$

следовательно, данное сравнение имеет два решения.

Пример 4. Решить сравнение $x^9-x^3+x-1\equiv 0(\mathrm{mod}\ 5)$.

Решение. Так как степень сравнения больше значения модуля, то необходимо заменить данное сравнение эквивалентным сравнением, степень которого меньше модуля 5. Для этого многочлен

$$x^9-x^3+x-1$$

разделим на x^5-x с остатком:

$$x^9-x^3+x-1=(x^5-x)(x^4+1)+(-x^3+2x-1).$$

Заменим левую часть данного сравнения остатком $-x^3+2x-1$ и получим эквивалентное сравнение данному, степень которого ниже числа 5:

$$-x^3+2x-1\equiv 0(\mathrm{mod}\ 5).$$

Умножив сравнение на число 4, получим сравнение со старшим коэффициентом равным 1:

$$x^3+3x-4\equiv 0(\mathrm{mod}\ 5).$$

Полученное сравнение имеет меньше трех решений, так как коэффициенты остатка от деления многочлена x^5-x на многочлен x^3+3x-4, равного $4x^2+8x-12$, не делятся на 5.

Далее, разложим многочлен x^3+3x-4 на множители

$$x^3+3x-4=(x-1)(x^2+x+4)$$

и заметим, что данное сравнение имеет единственное решение

$$x\equiv 1(\mathrm{mod}\ 5).$$

Пример 5. Найти однозначное положительное число, 31-я степень которого оканчивается цифрой 7.

Решение. Если обозначить искомое число за x, то для нахождения его потребуется решить сравнение

$$x^{31}\equiv 7(\mathrm{mod}\ 10),$$

где $(7,10)=1$.

По одному из свойств сравнения

$$a\equiv b(\mathrm{mod}\, m),$$

$(a,m)=(b,m)$, отсюда $(x,10)=1$, применив теорему Эйлера, получим сравнение

$$x^4\equiv 1(\mathrm{mod}\ 10).$$

Возведем левую и правую части сравнения в 7-ю степень, после чего придем к сравнению

$$x^{28}\equiv 1(\text{mod } 10).$$

Тогда сравнение

$$x^{31}\equiv 7(\text{mod } 10)$$

можно преобразовать следующим образом:

$$x^{31}= x^{28}x^3\equiv x^3(\text{mod } 10),$$

$$x^3\equiv 7(\text{mod } 10).$$

Так как $(x,10)=1$, то методом испытания вычетов 1, 3, 5, 7, 9 находим единственное решение $x\equiv 3(\text{mod } 10)$. Следовательно,

$$3^{31}\equiv 7(\text{mod } 10).$$

Теорема Вильсона. Для любого простого числа p имеет место сравнение:

$$(p\text{-}1)!+1\equiv 0(\text{mod } p).$$

Доказательство. Пусть $p=2$. Тогда $(2\text{-}1)!+1=2\equiv 0(\text{mod } 2)$.

Пусть теперь $p\geq 3$, т.е. p нечетно. Свободный член сравнения

$$f(x)=(x\text{-}1)(x\text{-}2)\ \ldots(x\text{-}(p\text{-}1))\equiv 0(\text{mod } p),$$

равный $(p\text{-}1)!=1\cdot 2\ \ldots(p\text{-}1)$, не делится на p. Классы $\overline{1}$, $\overline{2}$,..., $\overline{(p-1)}$ удовлетворяют этому сравнению, т. е. число решений сравнения равно его степени.

Рассмотрим равенство

$$x^{p\text{-}1}\text{-}1=f(x)\cdot 1+r(x),$$

где $r(x)$ – остаток от деления x^{p-1} на $f(x)$. Тогда, согласно ***Теореме 5,*** все коэффициенты остатка

$$r(x)=(x^{p\text{-}1}\text{-}1)\text{-}(x\text{-}1)(x\text{-}2)\ \ldots\ (x\text{-}(p\text{-}1))$$

делятся на p. В частности, на p делится свободный член $r(x)$, равный по абсолютной величине $(p\text{-}1)!+1$.

УПРАЖНЕНИЯ

1. Заменить данные сравнения равносильными им сравнениями со старшим коэффициентами, равными единице:

a) $5x^4\text{-}3x^3+2x^2\text{-}x+5\equiv 0(\text{mod } 11)$;
b) $7x^5+4x^3\text{-}11x^2+8\equiv 0(\text{mod } 13)$;
c) $3x^6\text{-}2x^5+3x^3+2x^2\text{-}3\equiv 0(\text{mod } 7)$;
d) $13x^7+2x^6\text{-}7x^5+12x^4+6x^3\text{-}9x^2\text{-}2x+5\equiv 0(\text{mod } 15)$.

2. Заменить данные сравнения равносильными им сравнениями, степень которых ниже p, где p – модуль:

a) $x^{13}\text{-}3x^3\text{-}2x^2\text{-}7x+9\equiv 0(\text{mod } 11)$;
b) $x^8+4x^5\text{-}x^3+3\equiv 0(\text{mod } 5)$;
c) $x^9\text{-}3x^4+2x^3\text{-}x+3\equiv 0(\text{mod } 7)$;
d) $x^{14}\text{-}x^{12}+3x^5\text{-}6x^2+x+1\equiv 0(\text{mod } 11)$.

3. Выяснить, имеют ли сравнения максимальное число решений:

a) $x^3+x^2\text{-}1\equiv 0(\text{mod } 11)$;
b) $x^3+3x\text{-}1\equiv 0(\text{mod } 5)$;

c) $x^4-5x^2-3\equiv 0(\mathrm{mod}\ 7)$;

d) $3x^3-x^2+4x+1\equiv 0(\mathrm{mod}\ 7)$.

4. Решить сравнения:

a) $x^7-3x^6+x^5-x^3+4x^2-4x+2\equiv 0(\mathrm{mod}\ 5)$;

b) $x^8-x^4+2x-3\equiv 0(\mathrm{mod}\ 5)$;

c) $x^{14}-4x^{13}-x+6\equiv 0(\mathrm{mod}\ 13)$;

d) $3x^3-x^2+4x+1\equiv 0(\mathrm{mod}\ 7)$.

5. Разложить многочлен

$x^4+6x^3-3x^2+x+2\equiv 0(\mathrm{mod}\ 11)$.

на множители по модулю 13.

7. СРАВНЕНИЯ 2-Й СТЕПЕНИ ПО ПРОСТОМУ МОДУЛЮ

Сравнение 2-ой степени по простому модулю p имеет вид

$$c_0 x^2 + c_1 x + c_2 \equiv 0(\mathrm{mod}\ p).$$

В качестве модуля p берут нечетные простые числа. Будем рассматривать только случай, когда коэффициент c_0 не делится на p.

В ходе исследования и решения сравнения вида $c_0 x^2 + c_1 x + c_2 \equiv 0(\mathrm{mod}\ p)$ его заменяют эквивалентным сравнением вида $(x+c)^2 \equiv a(\mathrm{mod}\ p)$. Затем, заменяя $x+c$ на z, исследуют и решают сравнение вида $z^2 \equiv a(\mathrm{mod}\ p)$.

Сравнения вида $x^2 \equiv a(\mathrm{mod}\ p)$ могут не иметь решений.

Если же сравнение $x^2 \equiv a(\mathrm{mod}\ p)$ имеет решение $\overline{x}_0$, то решением будет также класс - $\overline{x}_0$, отличный от $\overline{x}_0$. Для составных модулей это утверждение неверно.

Пример 1. Имеет ли сравнение

$$x^2+3\equiv 0(\mathrm{mod}\ 7)$$

два различных сравнения?

Решение. Данное сравнение представим в виде

$$x^2\equiv -3(\mathrm{mod}\ 7)$$

и заменим число, стоящее в правой части сравнения положительным вычетом по модулю 7. Получим сравнение

$$x^2\equiv 4(\mathrm{mod}\ 7),$$

которое имеет два решения

$$x\equiv 2(\mathrm{mod}\ 7) \text{ и } x\equiv -2(\mathrm{mod}\ 7).$$

Определение 1. 1) Класс чисел по модулю p называется классом квадратичных вычетов по этому модулю, если для чисел a, принадлежащих этому классу, сравнение $x^2 \equiv a(\mathrm{mod}\ p)$ имеет два решения.

2) Класс чисел по модулю p называется классом квадратичных невычетов по этому модулю, если для чисел a, принадлежащих этому классу, сравнение $x^2 \equiv a(\mathrm{mod}\, p)$ не имеет решений.

Теорема (критерий Эйлера). 1) Чтобы число a было квадратичным вычетом по простому модулю p необходимо и достаточно, чтобы выполнялось сравнение $x^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\, p)$.

2) Чтобы число a было квадратичным невычетом по простому модулю p необходимо и достаточно, чтобы выполнялось сравнение $x^{\frac{p-1}{2}} \equiv -1(\mathrm{mod}\, p)$.

Определение 2. Пусть p – простое число, p>2 . Символом Лежандра $\left(\frac{a}{p}\right)$ обозначается +1 или -1, смотря по тому, будет ли a квадратичным вычетом или невычетом по модулю p.

Другими словами, $\left(\frac{a}{p}\right)$ равно +1, если сравнение $x^2 \equiv a(\mathrm{mod}\, p)$ имеет два решения, и $\left(\frac{a}{p}\right)$ равно -1, если это сравнение не имеет решений.

Свойства символа Лежандра

1. Если $a \equiv b(\mathrm{mod}\, p)$, то $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$.
2. $\left(\frac{a^2}{p}\right)=1$.
3. $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)(\mathrm{mod}\, p)$.
4. $\left(\frac{a_1 \ldots a_n}{p}\right)=\left(\frac{a_1}{p}\right)\ldots\left(\frac{a_n}{p}\right)$.
5. $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$.
6. Если p и q – различные нечетные простые числа, то $\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)$ (закон квадратичной взаимности).

Пример 1. С помощью критерия Эйлера среди чисел 2, 4, 5, 9 найти квадратичные вычеты по модулю 11.

Решение. Видно, что каждое число взаимно просто с модулем, поэтому критерий Эйлера применим. Как известно, если $(a,p)=1$ и $a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\, p)$, то a - квадратичный вычет по модулю p.

Для данных чисел имеем:

$2^5=32\equiv -1(\mathrm{mod}11)$;

$4^5=(32)^2\equiv 1(\mathrm{mod}11)$;

$$5^5=(25)^2 5\equiv 3^2 5=45\equiv 1(\mathrm{mod}11);$$
$$9^5\equiv(-2)^5=-32\equiv 1(\mathrm{mod}11).$$

Итак, числа 4, 5 и 9 являются квадратичными вычетами по модулю 11, а число 2 – квадратичный невычет.

Пример 2. Решить сравнение:

$$5x^2+x-7\equiv 0(\mathrm{mod}11)$$

Решение. Умножим обе части сравнения на число 20 взаимно простое с модулем 11. Получим сравнение:

$$100x^2+20x-140\equiv 0(\mathrm{mod}11),$$

или

$$(10x+1)^2\equiv 141(\mathrm{mod}11).$$

Обозначим $10x+1$ через z. итак $z^2\equiv 141(\mathrm{mod}\ 11)$, или $z^2\equiv 9(\mathrm{mod}\ 11)$.

Решим это сравнение методом испытания вычетов. Испытывая числа 0, 1, 2, …, 10, видим, что сравнение имеет решения: $z=3$ *и* $z=8$, т. е. удовлетворяется при $z=2+11t$ и $z=8+11t$. Так как $z=10x+1$, то $x=\dfrac{z-1}{10}$, т. е. $x_1=\dfrac{1+11t}{10}$ и $x_2=\dfrac{7+11t}{10}$; при $t=9$ имеем $x_1=10$ и при $t=3$ имеем $x_2=4$.

Следовательно, данное сравнение имеет решения:

$$x\equiv 4(\mathrm{mod}11) \text{ и } x\equiv 10(\mathrm{mod}11).$$

Пример 3. С помощью символа Лежандра установить, имеет ли решение сравнение: $x^2\equiv 404(\mathrm{mod}\ 523)$.

Решение. Если символ Лежандра $\left(\dfrac{a}{p}\right)=1$, то сравнение $x^2\equiv a(\mathrm{mod}\,p)$ имеет два решения. Вычислим символ Лежандра $\left(\dfrac{404}{523}\right)$. Для этого воспользуемся свойством: $\left(\dfrac{a^2b}{p}\right)=\left(\dfrac{b}{p}\right)$, откуда $\left(\dfrac{2^2 101}{523}\right)=\left(\dfrac{101}{523}\right)$. Применим закон взаимности $\left(\dfrac{p}{q}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\dfrac{q}{p}\right)$:

$\left(\dfrac{101}{523}\right)=(-1)^{\frac{101-1}{2}\cdot\frac{523-1}{2}}\left(\dfrac{523}{101}\right)=(-1)^{50\cdot 261}\left(\dfrac{523}{101}\right)=\left(\dfrac{523}{101}\right)$. Далее используем свойство: если $a\equiv b(\mathrm{mod}\,p)$, то $\left(\dfrac{a}{p}\right)=\left(\dfrac{b}{p}\right)$. Следовательно, $\left(\dfrac{523}{101}\right)=\left(\dfrac{18}{101}\right)$, откуда $\left(\dfrac{18}{101}\right)=\left(\dfrac{2}{101}\right)$. Далее применяя свойство $\left(\dfrac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$, получаем $\left(\dfrac{2}{101}\right)=(-1)^{\frac{101^2-1}{8}}=1$.

Так как $\left(\frac{404}{523}\right)=1$, то сравнение $x^2 \equiv 404 (\mathrm{mod}\ 523)$ имеет два решения.

УПРАЖНЕНИЯ

1. С помощью критерия Эйлера установить, какие из чисел 3, 5, 7, 8, 11 являются квадратичными вычетами по модулю 13.

2. С помощью критерия Эйлера установить, какие из чисел 5, 6. 7, 8, 10 являются квадратичными невычетами по модулю 17.

3. Доказать, что для символа Лежандра справедливо свойство $\left(\frac{q^n}{p}\right)=\left(\frac{q}{p}\right)^n$.

4. С помощью символа Лежандра установить, имеют ли решения сравнения:

a) $x^2 \equiv 104 (\mathrm{mod} 321)$;

b) $x^2 \equiv 219 (\mathrm{mod} 383)$;

c) $x^2 \equiv 231 (\mathrm{mod} 101)$;

d) $x^2 \equiv 65 (\mathrm{mod} 193)$.

5. Символ Якоби $\left(\frac{a}{m}\right)$ для нечетного $m=p_1 p_2 \ldots p_k$, где p_i – числа простые, среди которых могут быть и равные, и $(a, m)=1$, определяется равенством

$$\left(\frac{a}{m}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a_n}{p_k}\right),$$

где $\left(\frac{a}{p_i}\right)$ - символы Лежандра. Доказать, что символ Якоби обладает всеми свойствами символа Лежандра.

6. Применить символ Якоби к исследованию уравнений:

a) $x^2 \equiv 903 (\mathrm{mod} 2111)$;

b) $x^2 \equiv 219 (\mathrm{mod} 383)$;

c) $x^2 \equiv 7 (\mathrm{mod} 2003)$.

7. Решить уравнение $\left(\frac{a}{21}\right)=1$, где $\left(\frac{a}{21}\right)$ - символ Якоби.

8. ПЕРВООБРАЗНЫЕ КОРНИ

Определение 1. Показателем числа a по модулю m (обозначается $P_m(a)$ или $P(a)$ при фиксированном m) при условии $(a, m)=1$ называется наименьший положительный показатель степени a, сравнимый с единицей по модулю m.

Согласно этому определению, $P(a)$ –это наименьшее положительное число, такое, что $a^{P(a)}\equiv 1(\mathrm{mod}\ m)$.

Теорема 1. Если $b\equiv a(\mathrm{mod}\ m)$, то $P(b)=P(a)$.

Согласно этой теореме для всех чисел, принадлежащих одному и тому же классу показатель по данному модулю одинаков.

По теореме Эйлера $a^{\varphi(m)}\equiv 1(\mathrm{mod}\ m)$, следовательно, $\varphi(m)\vdots P(a)$.

Пример 1. Найти какому показателю принадлежит число 7 по модулю 16.

Решение. Так как числа 7 и 16 взаимно простые, то по определению показателя, будем искать наименьшее натуральное число z, удовлетворяющее сравнению

$$7^z\equiv 1(\mathrm{mod}\ 16),$$

среди делителей числа $\varphi(16)$.

В данном случае имеем:

$$\varphi(16)=\varphi(2^4)=8;$$

делителями 8 являются числа 1, 2, 4, 8; получим:

$$7^1\equiv 7(\mathrm{mod}\ 16),\ 7^2=49\equiv 1(\mathrm{mod}\ 16),$$

следовательно, число 7 принадлежит показателю 2 по модулю 16.

Определение 2. Порядком класса вычетов $\bar{a}$, взаимно простого с модулем m, называют наименьшее натуральное число δ, такое, что $\bar{a}^{\delta}=\bar{1}$.

Пример 2. Найти порядок класса вычетов $\bar{5}$ по модулю 13.

Решение. Так как $(5, 13)=1$, то $\bar{5}^{\delta}=\bar{1}$. Число δ есть показатель класса $\bar{5}$ по модулю 13. Найдем δ среди чисел 1, 2, 3, 4, 6 и 12, которые являются делителями $\varphi(13)=13-1=12$:

$$5^1\equiv 5(\mathrm{mod}\ 13),$$
$$5^2\equiv -1(\mathrm{mod}\ 13),$$
$$5^3\equiv 8(\mathrm{mod}\ 13),$$
$$5^4\equiv 1(\mathrm{mod}\ 13).$$

Следовательно, $\delta=4$.

Определение 3. Если δ есть показатель числа a по простому модулю p и $\delta=\varphi(p)=p-1$, то a называется первообразным корнем по модулю p.

Пример 3. Найти показатель, которому принадлежит число 5 по модулю 23.

Решение. Найдем наименьший показатель δ числа 5 среди делителей числа $\varphi(23)=23-1=22$, чтобы сравнение $5^{\delta}\equiv 1(\mathrm{mod}\ 23)$ было справедливо:

$$5^1\equiv 5(\mathrm{mod}\ 23),$$
$$5^2\equiv 2(\mathrm{mod}\ 23),$$
$$5^{11}\equiv 22(\mathrm{mod}\ 23),$$
$$5^{22}\equiv 1(\mathrm{mod}\ 23).$$

Итак, $\delta=22=\varphi(23)$. Следовательно, число 5 является первообразным корнем по модулю 23.

Определение 4. Первообразным корнем по простому модулю p называется класс вычетов $\overline{g}$ по этому модулю, порядок которого равен p-1.

Теорема 2. Если число a принадлежит показателю δ по простому модулю p, то все числа, принадлежащие показателю δ находятся среди чисел a^1, a^2,..., a^δ, у которых показатели взаимно простые с δ.

Следуя этой ***Теореме***, существует $\varphi(\delta)$ различных классов чисел, принадлежащих показателю δ.

Теорема 3. Пусть $\varphi(p)=p-1=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$. Для того чтобы класс $\overline{g}$, взаимно простой с p был первообразным корнем, необходимо и достаточно, чтобы g не удовлетворял ни одному из сравнений:

$$g^{\frac{p-1}{p_1}} \equiv 1(\mathrm{mod}\, p),\ g^{\frac{p-1}{p_2}} \equiv 1(\mathrm{mod}\, p),\ \ldots,\ g^{\frac{p-1}{p_k}} \equiv 1(\mathrm{mod}\, p).$$

Если p – простое нечетное число, то существует $\varphi(p\text{-}1)$ первообразных корней по модулю p.

Пример 4. Найти все первообразные корни по модулю 31.

Решение. По определению число g будет первообразным корнем по модулю 31, если его порядок равен $\varphi(31)=30$.

Найдем наименьший первообразный корень по модулю 31. Для этого воспользуемся предыдущей ***Теоремой***: пусть $\varphi(31)=30=2^1\cdot 3\cdot 5$, тогда число g является первообразным корнем по модулю 31 тогда и только тогда, когда g не удовлетворяет ни одному из сравнений:

$$g^{\frac{31-1}{2}} \equiv 1(\mathrm{mod}\, 31),\ g^{\frac{31-1}{3}} \equiv 1(\mathrm{mod}\, 31),\ g^{\frac{31-1}{5}} \equiv 1(\mathrm{mod}\, 31)$$

или

$$g^{15} \equiv 1(\mathrm{mod}\, 31),\ g^{10} \equiv 1(\mathrm{mod}\, 31),\ g^{6} \equiv 1(\mathrm{mod}\, 31).$$

В качестве значений g будем выбирать наименьшие положительные вычеты по модулю 31.

Пусть g=1. Так как $1^6 \equiv 1(\mathrm{mod}\, 31)$, то число 1 не является первообразным корнем по модулю 31.

Пусть g=2. Получаем:

$$2^6 \equiv 64 \equiv 2(\mathrm{mod}\, 31),$$

$$2^{10} = 2^6 \cdot 2^4 \equiv 2\cdot 16 \equiv 32 \equiv 1(\mathrm{mod}\, 31).$$

Значит, число 2 не является первообразным корнем по модулю 31.

Пусть g=3. Получаем:

$$3^6 = 729 \equiv 16(\mathrm{mod}\, 31),$$

$$3^{10} = 3^6 \cdot 3^4 \equiv 16\cdot 19 \equiv 25(\mathrm{mod}\, 31),$$

$$3^{15} = 3^{10}3^5 \equiv 25\cdot 26 \equiv -6\cdot(-5) = 30 \equiv -1(\mathrm{mod}\, 31).$$

Следовательно, число 3 является наименьшим первообразным корнем по модулю 31.

Все остальные первообразные корни по данному модулю будем искать в виде наименьших положительных вычетов степеней числа 3, т. е. в виде 3^s, где

$(s,p\text{-}1)=1$. Число всех первообразных корней по модулю 31 равно $\varphi(p\text{-}1)=\varphi(30)=\varphi(2\cdot3\cdot5)=1\cdot2\cdot4=8$. Таким образом, первообразными корнями по модулю 31 являются числа $3^1, 3^7, 3^{11}, 3^{13}, 3^{17}, 3^{19}, 3^{23}, 3^{29}$, где

$$3^1\equiv3(\text{mod }31),$$
$$3^7\equiv17(\text{mod }31),$$
$$3^{11}\equiv8(\text{mod }31),$$
$$3^{13}\equiv10(\text{mod }31),$$
$$3^{17}\equiv4(\text{mod }31),$$
$$3^{19}\equiv36(\text{mod }31),$$
$$3^{23}\equiv6(\text{mod }31),$$
$$3^{29}\equiv21(\text{mod }31).$$

Итак, первообразными корнями по модулю 31 являются числа: 3, 4, 6, 8, 10, 17, 21, 36, иначе классы вычетов по модулю 31: $\overline{3}$, $\overline{4}$, $\overline{6}$, $\overline{8}$, $\overline{10}$, $\overline{17}$, $\overline{21}$, $\overline{36}$.

УПРАЖНЕНИЯ

1.Какому показателю принадлежат:

a) число 5 по модулю 12,
b) число 6 по модулю 17,
c) число 3 по модулю 17,
d) число 11 по модулю 31.

2. Найти все показатели, которым принадлежат числа:

a) по модулю 11,
b) по модулю 17,
c) по модулю 12,
d) по модулю 15.

3. Найти наименьший первообразный корень:

a) модулю 13,
b) по модулю 19,
c) по модулю 29,
d) по модулю 43.

4. Найти все первообразные корни:

a) по модулю 23,
b) по модулю 37,
c) по модулю 41,
d) по модулю 53.

5. Зная, что число 2 есть первообразный корень по модулю 37, показать справедливость сравнения

$$2^{18}\equiv6^2(\text{mod }37).$$

6. Найти $P_m(m\text{-}1)$.

7. Доказать, что модуль 8 не имеет первообразных корней. *Указание*: испытать приведенную систему вычетов.

8. Показать, что если $(a, p)=1$, где p - простое число, $a^{2k}\equiv1(\text{mod }p)$ и число a принадлежит показателю $2k$ по модулю p, то $a^k\equiv-1(\text{mod }p)$. *Указание.* Исследовать сравнение $(a^k\text{-}1)(a^k+1)\equiv0(\text{mod }p)$.

9. Доказать, что если число a – первообразный корень простого модуля p, то a^k, где $(k,p\text{-}1)=1$, также является первообразным корнем по модулю p.

10.Доказать, что если числа a и b являются первообразными корнями по простому модулю $p>2$, то произведение ab не может быть первообразным корнем по модулю p.

11. Доказать, что первообразный корень g по простому модулю p есть квадратичный невычет по тому же модулю.

12. Число 43 – первообразный корень по модулю 89; показать, что сравнение

$$x^2 \equiv 43 (\mathrm{mod}\ 89)$$

не имеет решений.

13. Показать, что среди первообразных корней по простому модулю $p>2$ не может быть полных квадратов.

9. ИНДЕКСЫ

Определение 1. Если первообразный корень g по простому модулю p и для числа a, где $(a, p)=1$, имеет место сравнение

$$a \equiv g^k (\mathrm{mod}\ p),\ k \geq 0,$$

то k называется индексом числа a по модулю p при основании g.

Для краткости при фиксированном модуле p и основании g будем записывать это в виде $k=\mathrm{ind}\ a$.

Индекс числа a является также индексом и всех чисел из $\overline{a}$.

Основные свойства индексов

$$\mathrm{ind}ab \equiv \mathrm{ind}a + \mathrm{ind}b (\mathrm{mod}\ p-1),$$

$$\mathrm{ind}\frac{a}{b} \equiv \mathrm{ind}a - \mathrm{ind}b (\mathrm{mod}\ p-1),$$

$$\mathrm{ind}a^n \equiv n\mathrm{ind}a (\mathrm{mod}\ p-1),$$

$$\mathrm{ind}1 \equiv 0 (\mathrm{mod}\ p-1),$$

$$\mathrm{ind}g \equiv 1 (\mathrm{mod}\ p-1).$$

Пример 1. Составить таблицу индексов по модулю 31.

Решение. В предыдущем пункте в ***Примере 4*** найден наименьший первообразный корень по модулю 31. Это число 3. Данное число принимаем за основание индексов. Находим наименьшие положительные вычеты по модулю 31, заставляя пробегать показатели степени числа 3 последовательно все значения от 0 до 30. Имеем:

$3^0 \equiv 1 (\mathrm{mod}\ 31)$, ind 1=0;
$3^1 \equiv 3 (\mathrm{mod}\ 31)$, ind 3=1;
$3^2 \equiv 9 (\mathrm{mod}\ 31)$, ind 2=2;
$3^3 \equiv 27 (\mathrm{mod}\ 31)$, ind 27=3;
$3^4 \equiv 19 (\mathrm{mod}\ 31)$, ind 19=4;
$3^5 \equiv 26 (\mathrm{mod}\ 31)$, ind 26=5;
$3^6 \equiv 16 (\mathrm{mod}\ 31)$, ind 16=6;
$3^7 \equiv 17 (\mathrm{mod}\ 31)$, ind 17=7;
$3^8 \equiv 20 (\mathrm{mod}\ 31)$, ind 20=8;
$3^9 \equiv 29 (\mathrm{mod}\ 31)$, ind29=9;
$3^{10} \equiv 25 (\mathrm{mod}\ 31)$, ind 25=10;
$3^{11} \equiv 13 (\mathrm{mod}\ 31)$, ind 13=11;
$3^{12} \equiv 8 (\mathrm{mod}\ 31)$, ind 8=12;
$3^{13} \equiv 24 (\mathrm{mod}\ 31)$, ind 24=13;

$3^{14}\equiv 10(\mathrm{mod}\ 31)$, ind 10=14;
$3^{15}\equiv 30(\mathrm{mod}\ 31)$, ind 30=15;
$3^{16}\equiv 26(\mathrm{mod}\ 31)$, ind 26=16;
$3^{17}\equiv 22(\mathrm{mod}\ 31)$, ind 22=17;
$3^{18}\equiv 4(\mathrm{mod}\ 31)$, ind 4=18;
$3^{19}\equiv 12(\mathrm{mod}\ 31)$, ind 12=19;
$3^{20}\equiv 5(\mathrm{mod}\ 31)$, ind 5=20;
$3^{21}\equiv 15(\mathrm{mod}\ 31)$, ind 15=21;
$3^{22}\equiv 14(\mathrm{mod}\ 31)$, ind 14=22;
$3^{23}\equiv 11(\mathrm{mod}\ 31)$, ind 11=23;
$3^{24}\equiv 2(\mathrm{mod}\ 31)$, ind 2=24;
$3^{25}\equiv 6(\mathrm{mod}\ 31)$, ind 6=25;
$3^{26}\equiv 18(\mathrm{mod}\ 31)$, ind 18=26;
$3^{27}\equiv 23(\mathrm{mod}\ 31)$, ind 23=27;
$3^{28}\equiv 7(\mathrm{mod}\ 31)$, ind 7=28;
$3^{29}\equiv 21(\mathrm{mod}\ 31)$, ind 21=29.

Полученные значения индексов сведем в таблицу, в которой число единиц откладывают по верхней строке, число десятков по первому столбцу. Данная таблица служит для нахождения индексов по числам.

N	0	1	2	3	4	5	6	7	8	9
0		0	24	1	18	20	25	28	12	2
1	14	23	19	11	22	21	6	7	26	4
2	8	29	17	27	13	10	5	3	16	9
3	15									

Можно составить таблицу для нахождения чисел по индексам.

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	19	26	16	17	20	29
1	25	13	8	24	10	30	28	22	4	12
2	5	15	14	11	2	6	18	23	7	21

Пример 2. Решить сравнение с помощью таблицы индексов

$$15x^4 \equiv 26(\mathrm{mod}\,29).$$

Решение. «Индексируем» левую и правую часть сравнения и получаем сравнение по новому модулю 28:

$$\mathrm{ind}\,15x^4 \equiv \mathrm{ind}\,26(\mathrm{mod}28).$$

Пользуясь свойствами индексов, получаем:

$$\mathrm{ind}\,15+4\mathrm{ind}\,x \equiv \mathrm{ind}\,26(\mathrm{mod}28)$$

или

$$4\mathrm{ind}\,x \equiv \mathrm{ind}\,26-\mathrm{ind}\,15(\mathrm{mod}28).$$

В таблице индексов по модулю 29 найдем значения ind15 и ind26; они соответственно равны 27 и 19. Обозначая ind$x=y$, переходим к решению сравнения первой степени:

$$4y\equiv -8(\mathrm{mod}\ 28).$$

Полученное сравнение имеет 4 решения:

$$y\equiv -2(\mathrm{mod}\ 28),$$
$$y\equiv 5(\mathrm{mod}\ 28),$$
$$y\equiv 12(\mathrm{mod}\ 28),$$
$$y\equiv 19(\mathrm{mod}\ 28).$$

Сделаем обратную замену в каждом из этих сравнений:

$$\mathrm{ind}\ x\equiv -2\equiv 26(\mathrm{mod}\ 28),$$
$$\mathrm{ind}\ x\equiv 5(\mathrm{mod}\ 28),$$
$$\mathrm{ind}\ x\equiv 12(\mathrm{mod}\ 28),$$
$$\mathrm{ind}\ x\equiv 19(\mathrm{mod}\ 28);$$

и используя таблицу для нахождения числа по индексу, получим окончательные решения данного сравнения:

$$x\equiv 22(\mathrm{mod}\ 29),$$
$$x\equiv 3(\mathrm{mod}\ 29),$$
$$x\equiv 7(\mathrm{mod}\ 29),$$
$$x\equiv 26(\mathrm{mod}\ 29).$$

Пример 3. Решить сравнение с помощью таблицы индексов

$$17^x\equiv 7(\mathrm{mod}53).$$

Решение. «Индексируем» левую и правую часть сравнения и получаем сравнение по новому модулю 53:

$$\mathrm{ind}17^x\equiv \mathrm{ind}7(\mathrm{mod}\ 53).$$

Пользуясь свойствами индексов, получаем:

$$x\mathrm{ind}17\equiv \mathrm{ind}7(\mathrm{mod}\ 53).$$

В таблице индексов по модулю 53 найдем значения ind17 и ind7; они соответственно равны 10 и 14. Тогда исходное сравнение примет вид:

$$10x\equiv 14(\mathrm{mod}\ 53)$$

или

$$5x\equiv 7(\mathrm{mod}\ 53).$$

Так как (5,53)=1, данное сравнение имеет единственное решение, которое найдем, прибавив к его правой части один раз модуль 53:

$$5x\equiv 60(\mathrm{mod}\ 53),$$
$$x\equiv 12(\mathrm{mod}\ 53).$$

Пример 4. С помощью таблиц индексов найти остаток от деления 10^{10} на 71.

Решение. Обозначим искомый остаток через r, т. е.

$$10^{10}\equiv r(\mathrm{mod}\ 71).$$

Берем индексы от обеих частей сравнения:

$$10\mathrm{ind}10\equiv \mathrm{ind}\ r(\mathrm{mod}\ 70).$$

Из таблицы индексов для простого числа 71 находим, что ind10≡34(mod70), следовательно, 340≡ind r(mod 70), или ind r≡60(mod 70). Теперь из таблицы для нахождения числа по индексу по простому модулю 71 находим, что

$$r\equiv 30 \pmod{71}.$$

Таким образом, искомый остаток равен 30.

Пример 5. С помощью таблиц индексов найти показатель, которому принадлежит число 15 по модулю 79.

Решение. (15, 79)=1, а поэтому искомый показатель должен удовлетворять сравнению $15^{\delta}\equiv 1 \pmod{79}$.

Применяя свойства индексов и пользуясь таблицей индексов для простого числа 79, находим:

$$\delta \operatorname{ind} 15 \equiv \operatorname{ind} 1 \pmod{78},\quad 63\delta\equiv 0 \pmod{78},\quad 21\delta\equiv 0 \pmod{26};$$

наименьшее положительное значение δ=26, удовлетворяющее этому сравнению, будет являться искомым показателем.

УПРАЖНЕНИЯ

1. Составить таблицу индексов:
   a) по модулю 11,
   b) по модулю 19,
   c) по модулю 23,
   d) по модулю 31.
2. Решить сравнения при помощи таблицы индексов:
   a) $8x\equiv 26 \pmod{37}$,
   b) $x^2\equiv 3 \pmod{11}$,
   c) $13x^{12}\equiv 26 \pmod{31}$,
   d) $40x^{10}\equiv 3 \pmod{17}$,
   e) $13a^2-11\equiv 0 \pmod{29}$,
   f) $3x^6\equiv 7 \pmod{61}$,
   g) $3x^3\equiv 2 \pmod{37}$,
   h) $2^x\equiv 7 \pmod{19}$,
   i) $16^x\equiv 11 \pmod{43}$,
   j) $27^{x^2}\equiv 17 \pmod{31}$,
   k) $3^{x^2}\equiv 23 \pmod{29}$,
   l) $123^{x^2}\equiv 17 \pmod{47}$.
3. С помощью таблиц индексов найти остатки от деления:
   a) 89·78 на число 61,
   b) числа 15^{27} на число 59,
   c) 53·41·19 на число 89,
   d) числа 31^{124} на число 37.
4. Доказать, что индекс числа -1 по нечетному модулю p всегда равен $\frac{p-1}{2}$.
5. Обобщить критерий Эйлера на случай сравнения $x^n\equiv a \pmod{p}$, где a не сравнимо с нулем по данному модулю p (p>2).
6. Вывести формулу перехода от одной системы индексов к другой по данному модулю.

10. АРИФМЕТИЧЕСКИЕ ПРИЛОЖЕНИЯ ТЕОРИИ СРАВНЕНИЙ

Рассмотрим применение теории сравнений к вопросу об отыскании признаков делимости на числа взаимно простые с 10.

Теорема 1. Пусть $(m,10)=1$, $P_m(10)=k$ и N записано в десятичной системе счисления. Число N делится на m тогда и только тогда, когда на m делится сумма чисел, которые получаются при разбиении справа налево цифровой записи числа N на грани по k цифр в каждой грани.

Пример 1. 1) Признак делимости на 9. $P_9(10)=1$, $10^1\equiv1(\mathrm{mod}\ 9)$. Число делится на 9 тогда и только тогда, когда на 9 делится сумма его цифр.

2) Признак делимости на 11. $P_{11}(10)=2$, $10^2\equiv1(\mathrm{mod}\ 11)$. Число делится на 11 тогда и только тогда, когда на 11 делится сумма чисел, которые получаются при разбиении данного числа на грани по 2 цифры в каждой грани.

3) Признак делимости на 7. Так как $P_7(10)=6$: число делится или не делится на 7, смотря по тому делится или не делится ли на 7 сумма чисел, получающихся при разбиении числа на грани по 6 цифр в каждой грани.

Применять этот признак имеет смысл тогда, когда испытываемые числа велики.

Теорема 2. Пусть N записано в десятичной системе счисления. N делится на 2^n (на 5^n) тогда и только тогда, когда на 2^n (соответственно на 5^n) делится число, имеющее те же цифры, что и последние n цифр числа N.

Пример 2. Определить, делится ли число 6626221625 на 125.

Решение. $125=5^3$ и число 625, составленное из последних трех цифр, делится на 125. Следовательно, 6626221625 делится на 125.

Пример 3. Определить, делится ли число 1321936 на 4144.

Решение. $4144=2^4\cdot7\cdot37$. Заметим, что последние цифры исследуемого числа образуют число 1936, делящееся на 2^4. Следовательно, и само число 1321936 делится на 2^4. Разбивая число 1321936 на грани по шесть цифр, получаем:

$$1321936\equiv1+321936=321937=45991\cdot7(\mathrm{mod}\ 7),$$

так что данное число делится на 7. Так как $10^3\equiv1(\mathrm{mod}\ 37)$, то, разбивая на число 1321936 на грани по три цифры в каждой, получаем:

$$1321936\equiv1+321+936=1258=34\cdot37\equiv0(\mathrm{mod}\ 37),$$

так что число 1321936 делится на 37.

А значит, число 1321936 делится на 4144.

Предыдущие теоремы являются частным случаем применения способа Паскаля для отыскания признаков делимости.

Теорема (общий признак делимости Паскаля). Для того чтобы число N, записанное в g-ичной системе счисления в виде:

$$N=a_n g^n+a_{n-1}g^{n-1}+\ldots+a_1 g+a_0,$$

делилось на m необходимо и достаточно, чтобы число

$$Q=a_n r_n+a_{n-1}r_{n-1}+\ldots+a_1 r_1+a_0,$$

делилось на m, где r_i - абсолютно наименьшие вычеты соответствующих степеней gi по модулю m, $i=1, 2, \ldots, n$.

Следствие 1. Пусть m делитель числа g-1. Для того, чтобы число N, записанное в g- ичной системе счисления делилось на m, необходимо и достаточно, чтобы его сумма делилась на m.

Для чисел в десятичной системе счисления имеют место признаки делимости на 3 и на 9.

Следствие 2. Пусть m делитель числа g+1. Для того, чтобы число N, записанное в g- ичной системе счисления делилось на m, необходимо и достаточно, чтобы разность между суммами цифр на четных и на нечетных местах делилась на m.

Для чисел в десятичной системе счисления имет место признаки делимости на 11.

Теория сравнений дает способ проверки арифметических действий.

Выбираем некоторый модуль m и заменяем большие числа $a, b, c, \ldots$, над которыми надо производить действия (сложение, вычитание, умножение, деление, возведение в степень), наименьшими вычетами $a', b', c', \ldots$ по модулю m. Произведя действия над $a, b, c, \ldots$, точно такие же действия производим над $a', b', c', \ldots$ Если действия произведены правильно, то результаты этих действий над $a, b, c, \ldots$ и над $a', b', c', \ldots$ должны быть сравнимыми по модулю m.

Для этого обычно в качестве модуля выбирают m=9 и m=11.

При сложных вычислениях имеет смысл проводить две проверки: одну с помощью модуля 9, а другую с помощью модуля 11. В этом случае ошибка не будет замечена только, если она кратна 99.

Пример 4. Проверить правильность вычислений:

a) 135789+2468107=2603896;

b) 74646871-543289=74013529;

c) 2504759·142873=357862432607;

d) 5839131309:67377=85847;

e) $(3179)^3$= 32127104339.

Решение. a) Проверим правильность сложения с помощью модуля 9. Находим, что сумма цифр первого слагаемого $33\equiv6 \pmod 9$, а второго $28\equiv1 \pmod 9$. Сумма цифр результата сложения 34 отличается от 6+1=7 на число 27, кратное 9 , следовательно, результат вычисления верен.

b) Проверим правильность вычитания с помощью модуля 9. Находим, что сумма цифр уменьшаемого $43\equiv7 \pmod 9$, а вычитаемого $31\equiv4 \pmod 9$. Сумма цифр результата вычитания 31 отличается от 7-4=3 на число 28, не делящееся на 9, следовательно, результат вычисления неверен.

c) Проверим правильность умножения с помощью модуля 11. Знакопеременная сумма цифр первого множителя равна $18-14\equiv4 \pmod{11}$, второго – $10-15\equiv6 \pmod{11}$, а произведения $22-31=-9\equiv2 \pmod{11}$. Число, сравнимое со знакопеременной суммой цифр произведения, отличается от числа 4·6=24 на число 22, кратное 11. Таким образом, результат вычисления является правильным.

d) Проверим результат деления с помощью модулей 9 и 11, используя запись 5839131309=85847·67377. Сумма цифр делимого $42\equiv6 \pmod 9$, делителя $30\equiv3 \pmod 9$ и частного $32\equiv5 \pmod 9$. Произведение 3·5=15 отличается от 6 на число, кратное 9.

Знакопеременная сумма цифр делимого 22, делителя 2 и частного 14; 2·14=28 отличается от 22 на число, не кратное 11, так что результат неверен.

е) Проверим результат возведения в степень с помощью модуля 11. Знакопеременная сумма цифр основания 3-1+7-9=0. Соответствующая сумма для результата, равная 11, отличается от $0^3=0$ на 11,т.е. результат возведения в степень верен.

Теорема 4. Если $(b,10)=1$, то несократимая дробь $\frac{a}{b}$ обращается в чистую периодическую десятичную дробь с числом цифр в периоде равным $P_b(10)=\delta$, т.е. $\frac{a}{b}=0,(\alpha_1,\alpha_2, \dots , \alpha_\delta)$.

Пример 5. Найти число цифр в периоде десятичной дроби, в которую обращаются обыкновенные дроби со знаменателем равным 53.

Решение. Так как (53,10)=1, то любая несократимая дробь со знаменателем 53 разлагается в чистую периодическую дробь с числом цифр в периоде равным $P_{53}(10)$.

Испытывая делители числа $\varphi(53)=52$, имеем:

$$10^1\equiv 10(\mathrm{mod}\ 53),$$
$$10^2\equiv 47\equiv -6(\mathrm{mod}\ 53),$$
$$10^4\equiv 36\equiv -17(\mathrm{mod}\ 53),$$
$$10^{13}\equiv 1(\mathrm{mod}\ 53);$$

следовательно, показатель числа 10 по модулю 53 равен 13. А это означает, что период десятичной дроби со знаменателем равным 53 содержит тринадцать цифр.

Теорема 5. Если $b=2^\alpha 5^\beta b_1$, где $(b_1,10)=1$, то несократимая дробь $\frac{a}{b}$ обращается в смешанную периодическую десятичную дробь, в которой число цифр в периоде равно $P_{b_1}(10)$,а число цифр до периода $\mu=\{\alpha,\beta\}$.

Пример 6. Найти длину периода и число цифр до периода при обращении дроби $\frac{7}{2200}$ в бесконечную десятичную периодическую дробь.

Решение. Каноническим разложением числа 2200 будет $2^3\cdot 5^2\cdot 11$. Так как (11,10)=1, то для нахождения длины периода найдем $P_{11}(10)$:

$$10^1\equiv -1(\mathrm{mod}\ 11),$$
$$10^2\equiv 1(\mathrm{mod}\ 11).$$

Таким образом, число цифр до периода равно наибольшему показателю, с которым входят сомножители 2 и 5 в каноническое разложение знаменателя данной дроби, т.е. 3, а число цифр в периоде равно 2. Следовательно, $\frac{7}{2200}=0,003(18)$.

УПРАЖНЕНИЯ

1. Применить общий признак делимости Паскаля к установлению признаков делимости : a) на 6; b) на 8; c) на 12; d) на 15, 18 и 45.

2. Используя соответствующий признак делимости, проверить делимость чисел:

a) 45752850, 3138135, 5812560 на число 11;
b) 5258781, 15058 на число 33;
c) 240175, 9555 на число 65;
d) 45768519 на число 37;
e) 164164983 на число 111;
f) 20573685 на число 165.

3. Используя соответствующий признак делимости, проверить результат арифметических действий:

a) 457528507645+ 38135867=477566643512 с помощью модуля 9;
b) 25864·7613=196902632 с помощью модуля 11;
c) 90604878:159=568942 с помощью модуля 9;
d) $(7532)^4$=32184090840088576 с помощью модуля 11;

4. Найти все числа вида $\overline{13xy45z}$, делящиеся на 792.

5. Найти способ проверки «с помощью девятки» при извлечении корня любой степени. Найденным способом показать ошибочность записи:

$\sqrt[5]{371293} = 23.$

6. Найти длину периода и число цифр до периода при обращении дроби в бесконечную десятичную периодическую дробь:

a) $\frac{3}{14}$;
b) $\frac{3}{110}$;
c) $\frac{9}{550}$;
d) $\frac{17}{1230}$.

7. Найти знаменатель обыкновенной дроби вида $\frac{1}{m}$, которая представляется чистой периодической десятичной дробью с двумя цифрами в периоде.

8. Найти длину периода бесконечной десятичной дроби, заданной обыкновенной дробью $\frac{10}{17 \cdot 23}$.

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ ПО ТЕМЕ «РЕШЕНИЕ СРАВНЕНИЙ С НЕИЗВЕСТНОЙ ВЕЛИЧИНОЙ»

Вариант 1

1. Решить сравнения:
   a) методом Эйлера $5x \equiv 2(\mathrm{mod}8)$;
   b) методом подходящих дробей $13x \equiv 19(\mathrm{mod}215)$.
2. Решить неопределенное уравнение $73x+85y=-7$.
3. Решить систему сравнений

$$\begin{cases} 2x \equiv 7(\mathrm{mod}11), \\ 6x \equiv 3(\mathrm{mod}15), \\ x \equiv 2(\mathrm{mod}19). \end{cases}$$

4. Заменить данное сравнение равносильным, степень которого ниже p, где p - модуль

$$x^{14} - x^{12} + 3x^5 - 6x^2 + x + 1 \equiv 0(\mathrm{mod}11).$$

5. С помощью символа Лежандра установить, имеет ли решение сравнение

$$x^2 \equiv 42(\mathrm{mod}251).$$

Вариант 2

1. Решить сравнения:
   a) методом Эйлера $7x \equiv 2(\mathrm{mod}13)$;
   b) методом подходящих дробей $41x \equiv 32(\mathrm{mod}101)$.
2. Решить неопределенное уравнение $253x-449y=3$.
3. Решить систему сравнений

$$\begin{cases} 2x \equiv 3(\mathrm{mod}5), \\ 3x \equiv 5(\mathrm{mod}11), \\ 3x \equiv 12(\mathrm{mod}15). \end{cases}$$

4. Решить сравнение

$$x^{14} - 4x^{13} - x + 6 \equiv 0(\mathrm{mod}13).$$

5. С помощью символа Лежандра установить, имеет ли решение сравнение

$$x^2 \equiv 30(\mathrm{mod}269).$$

Вариант 3

1. Решить сравнения:
   a) методом Эйлера $5x \equiv 4(\mathrm{mod}7)$;
   b) методом подходящих дробей $25x \equiv 17(\mathrm{mod}151)$.
2. Решить неопределенное уравнение $172x+152y=-300$.
3. Решить систему сравнений

$$\begin{cases} 7x \equiv 9(\mathrm{mod}12), \\ x \equiv 6(\mathrm{mod}15), \\ 3x \equiv 5(\mathrm{mod}127). \end{cases}$$

4. Разложить на множители многочлен $x^4 + 6x^3 - 3x^2 + x + 2$ по модулю *13*.
5. С помощью символа Лежандра установить, имеет ли решение сравнение

$$x^2 \equiv 26(\mathrm{mod}241).$$

Вариант 4

1. Решить сравнения:
   a) методом Эйлера $3x \equiv 5(\mathrm{mod}11)$;
   b) методом подходящих дробей $23x \equiv 14(\mathrm{mod}109)$.
2. Решить неопределенное уравнение $24x-56y=72$.
3. Решить систему сравнений

$$\begin{cases} 7x \equiv 3(\mathrm{mod}9), \\ 3x \equiv 9(\mathrm{mod}12), \\ x \equiv 11(\mathrm{mod}13). \end{cases}$$

4. Заменить данное сравнение равносильным, степень которого ниже p, где p - модуль

$$x^{10} + 3x^5 - 4x^3 + x^2 - 3 \equiv 0(\mathrm{mod}7).$$

5. С помощью символа Лежандра установить, имеет ли решение сравнение

$$x^2 \equiv 20(\mathrm{mod}101).$$

Вариант 5

1. Решить сравнения:
   a) методом Эйлера $3x \equiv 4(\mathrm{mod}7)$;
   b) методом подходящих дробей $11x \equiv 26(\mathrm{mod}107)$.
2. Решить неопределенное уравнение $162x+104y=-10$.
3. Решить систему сравнений

$$\begin{cases} 9x \equiv 3(\mathrm{mod}14), \\ 4x \equiv 20(\mathrm{mod}18), \\ x \equiv 5(\mathrm{mod}11). \end{cases}$$

4. Решить сравнение

$$x^{12} + 2x^{11} - 2x - 1 \equiv 0(\mathrm{mod}11).$$

5. С помощью символа Лежандра установить, имеет ли решение сравнение

$$x^2 \equiv 65(\mathrm{mod}193).$$

Вариант 6

1. Решить сравнения:

a) методом Эйлера $2x \equiv 9(\mathrm{mod}15)$;

b) методом подходящих дробей $45x \equiv 8(\mathrm{mod}113)$.

2. Решить неопределенное уравнение $39x$-$45y$=21.

3. Решить систему сравнений

$$\begin{cases} 5x \equiv 3(\mathrm{mod}17), \\ x \equiv 1(\mathrm{mod}12), \\ 8x \equiv 2(\mathrm{mod}6). \end{cases}$$

4. Разложить на множители многочлен $x^4 - 4x^3 + 4x - 1$ по модулю *7*.

5. С помощью символа Лежандра установить, имеет ли решение сравнение

$$x^2 \equiv 33(\mathrm{mod}179).$$

Вариант 7

1. Решить сравнения:

a) методом Эйлера $4x \equiv 7(\mathrm{mod}9)$;

b) методом подходящих дробей $19x \equiv 42(\mathrm{mod}163)$.

2. Решить неопределенное уравнение $107x$+$84y$=1.

3. Решить систему сравнений

$$\begin{cases} 2x \equiv 7(\mathrm{mod}113), \\ 7x \equiv 8(\mathrm{mod}9), \\ 3x \equiv 4(\mathrm{mod}19). \end{cases}$$

4. Заменить данное сравнение равносильным, степень которого ниже *p*, где *p* - модуль

$$x^9 - 3x^4 + 2x^3 - x + 3 \equiv 0(\mathrm{mod}7).$$

5. С помощью символа Лежандра установить, имеет ли решение сравнение

$$x^2 \equiv 28(\mathrm{mod}251).$$

Вариант 8

1. Решить сравнения:

a) методом Эйлера $7x \equiv 2(\mathrm{mod}11)$;

b) методом подходящих дробей $12x \equiv 31(\mathrm{mod}137)$.

2. Решить неопределенное уравнение $37x$-$256y$=1.

3. Решить систему сравнений

$$\begin{cases} x \equiv 2(\mathrm{mod}103), \\ 3x \equiv 9(\mathrm{mod}21), \\ 2x \equiv 6(\mathrm{mod}12). \end{cases}$$

4. Решить сравнение $x^8 - 2x^7 + 3x^6 + x^5 - 2x^2 - x - 3 \equiv 0(\mathrm{mod}5)$.

5. С помощью символа Лежандра установить, имеет ли решение сравнение

$$x^2 \equiv 12(\mathrm{mod}269).$$

Вариант 9

1. Решить сравнения:
   a) методом Эйлера $4x \equiv 5(\mathrm{mod}13)$;
   b) методом подходящих дробей $8x \equiv 17(\mathrm{mod}127)$.
2. Решить неопределенное уравнение $571x+359y=-10$.
3. Решить систему сравнений

$$\begin{cases} 2x \equiv 3(\mathrm{mod}7), \\ 3x \equiv 5(\mathrm{mod}131), \\ 2x \equiv 10(\mathrm{mod}14). \end{cases}$$

4. Разложить на множители многочлен $x^4 - 3x^3 - x + 4$ по модулю *7*.
5. С помощью символа Лежандра установить, имеет ли решение сравнение

$$x^2 \equiv 48(\mathrm{mod}193).$$

Вариант 10

1. Решить сравнения:
   a) методом Эйлера $5x \equiv 12(\mathrm{mod}13)$;
   b) методом подходящих дробей $6x \equiv 31(\mathrm{mod}149)$.
2. Решить неопределенное уравнение $60x-91y=2$.
3. Решить систему сравнений

$$\begin{cases} 2x \equiv 3(\mathrm{mod}5), \\ 24x \equiv 14(\mathrm{mod}26), \\ 3x \equiv 5(\mathrm{mod}11). \end{cases}$$

4. Заменить данное сравнение равносильным, степень которого ниже p, где p - модуль

$$x^8 - 2x^7 + 3x^6 + x^5 - 2x^2 - x - 3 \equiv 0(\mathrm{mod}5).$$

5. С помощью символа Лежандра установить, имеет ли решение сравнение

$$x^2 \equiv 56(\mathrm{mod}241).$$

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ ПО ТЕМЕ «АРИФМЕТИЧЕСКИЕ ПРИЛОЖЕНИЯ ТЕОРИИ СРАВНЕНИЙ»

Вариант 1

1. С помощью числа 9 проверить результат арифметических действий 115403365:23845=48417.

2. Найти длину периода и количество цифр между запятой и периодом десятичной дроби, в которую обращается обыкновенная несократимая дробь со знаменателем 860.

3. Используя понятие числа, принадлежащего показателю, найти длину периода при обращении в десятичные дроби обыкновенных несократимых дробей со знаменателем 53.

4. Используя таблицы индексов, найти остаток от деления числа 19^{32} на число 67.

5. Используя соответствующий признак делимости, проверить делимость чисел 90585 и 254925 на число 165.

6. С помощью таблиц индексов найти показатель, которому принадлежит число 23 по модулю 53.

7. С помощью таблиц индексов решить сравнение $5x^3 \equiv 38 (\mathrm{mod}\ 47)$.

8. Найти все первообразные корни по модулю 71.

Вариант 2

1. С помощью числа 9 проверить результат арифметических действий 421767:3429=123.

2. Найти длину периода и количество цифр между запятой и периодом десятичной дроби, в которую обращается обыкновенная несократимая дробь со знаменателем 850.

3. Используя понятие числа, принадлежащего показателю, найти длину периода при обращении в десятичные дроби обыкновенных несократимых дробей со знаменателем 71.

4. Используя таблицы индексов, найти остаток от деления числа 11^{37} на число 61.

5. Используя соответствующий признак делимости, проверить делимость чисел 111888, 121878 и 145854 на число 111.

6. С помощью таблиц индексов найти показатель, которому принадлежит число 15 по модулю 47.

7. С помощью таблиц индексов решить сравнение $2x^4 \equiv 33 (\mathrm{mod}\ 43)$.

8. Найти наименьший первообразный корень по модулю 67.

Вариант 3

1. С помощью числа 9 проверить результат арифметических действий 1042·1011=1053462.

2. Найти длину периода и количество цифр между запятой и периодом десятичной дроби, в которую обращается обыкновенная несократимая дробь со знаменателем 620.

3. Используя понятие числа, принадлежащего показателю, найти длину периода при обращении в десятичные дроби обыкновенных несократимых дробей со знаменателем 89.

4. Используя таблицы индексов, найти остаток от деления числа 7^{23} на число 59.

5. Используя соответствующий признак делимости, проверить делимость чисел 121878, 141858 и 145854 на число 37.

6. С помощью таблиц индексов найти показатель, которому принадлежит число 19 по модулю 43.

7. С помощью таблиц индексов решить сравнение $7x^3 \equiv 14 (\mathrm{mod}\ 41)$.

8. Найти наименьший первообразный корень по модулю 61.

Вариант 4

1. С помощью числа 9 проверить результат арифметических действий

$$4371 \cdot 1243 = 5433153.$$

2. Найти длину периода и количество цифр между запятой и периодом десятичной дроби, в которую обращается обыкновенная несократимая дробь со знаменателем 208.

3. Используя понятие числа, принадлежащего показателю, найти длину периода при обращении в десятичные дроби обыкновенных несократимых дробей со знаменателем 83.

4. Используя таблицы индексов найти остаток от деления числа 17^{19} на число 53.

5. Используя соответствующий признак делимости, проверить делимость чисел 11934, 52434 и 111888 на число 54.

6. С помощью таблиц индексов найти показатель, которому принадлежит число 17 по модулю 41.

7. С помощью таблиц индексов решить сравнение $3x^5 \equiv 16 (\mathrm{mod}\ 31)$.

8. Найти наименьший первообразный корень по модулю 59.

Вариант 5

1. С помощью числа 9 проверить результат арифметических действий

$$42932 - 18265 = 24667.$$

2. Найти длину периода и количество цифр между запятой и периодом десятичной дроби, в которую обращается обыкновенная несократимая дробь со знаменателем 210.

3. Используя понятие числа, принадлежащего показателю, найти длину периода при обращении в десятичные дроби обыкновенных несократимых дробей со знаменателем 97.

4. Используя таблицы индексов, найти остаток от деления числа 31^{18} на число 37.

5. Используя соответствующий признак делимости, проверить делимость чисел 52434, 79974 и 111888 на число 27.

6. С помощью таблиц индексов найти показатель, которому принадлежит число 10 по модулю 37.

7. С помощью таблиц индексов решить сравнение $2x^6 \equiv 5 (\mathrm{mod}\ 31)$.

8. Найти наименьший первообразный корень по модулю 83.

Вариант 6

1. С помощью числа 9 проверить результат арифметических действий

37918-13207=24711.

2. Найти длину периода и количество цифр между запятой и периодом десятичной дроби, в которую обращается обыкновенная несократимая дробь со знаменателем 760.

3. Используя понятие числа, принадлежащего показателю, найти длину периода при обращении в десятичные дроби обыкновенных несократимых дробей со знаменателем 59.

4. Используя таблицы индексов, найти остаток от деления числа 29^{17} на число 41.

5. Используя соответствующий признак делимости, проверить делимость чисел 3038035 и 3539635 на число 65.

6. С помощью таблиц индексов найти показатель, которому принадлежит число 8 по модулю 31.

7. С помощью таблиц индексов решить сравнение $23x^3 \equiv 58 (\mathrm{mod}\ 97)$.

8. Найти наименьший первообразный корень по модулю 79.

Вариант 7

1. С помощью числа 9 проверить результат арифметических действий

115403365:23845=48417.

2. Найти длину периода и количество цифр между запятой и периодом десятичной дроби, в которую обращается обыкновенная несократимая дробь со знаменателем 385.

3. Используя понятие числа, принадлежащего показателю, найти длину периода при обращении в десятичные дроби обыкновенных несократимых дробей со знаменателем 47.

4. Используя таблицы индексов, найти остаток от деления числа 17^{19} на число 53.

5. Используя соответствующий признак делимости, проверить делимость чисел 52434, 79974 и 111888 на число 27.

6. С помощью таблиц индексов найти показатель, которому принадлежит число 8 по модулю 31.

7. С помощью таблиц индексов решить сравнение $3x^5 \equiv 18 (\mathrm{mod}\ 71)$.

8. Найти наименьший первообразный корень по модулю 73.

Вариант 8

1. С помощью числа 9 проверить результат арифметических действий

421767:3429=123.

2. Найти длину периода и количество цифр между запятой и периодом десятичной дроби, в которую обращается обыкновенная несократимая дробь со знаменателем 410.

3. Используя понятие числа, принадлежащего показателю, найти длину периода при обращении в десятичные дроби обыкновенных несократимых дробей со знаменателем 67.

4. Используя таблицы индексов, найти остаток от деления числа 19^{19} на число 97.

5. Используя соответствующий признак делимости, проверить делимость чисел 86670, 79974 и 333777 на число 27.

6. С помощью таблиц индексов найти показатель, которому принадлежит число 16 по модулю 53.

7. С помощью таблиц индексов решить сравнение $3^{x^2} \equiv 25 (\mathrm{mod}\ 31)$.

8. Найти наименьший первообразный корень по модулю 89.

Вариант 9

1. С помощью числа 11 проверить результат арифметических действий
864368582:77=11225566.

2. Найти длину периода и количество цифр между запятой и периодом десятичной дроби, в которую обращается обыкновенная несократимая дробь со знаменателем 510.

3. Используя понятие числа, принадлежащего показателю, найти длину периода при обращении в десятичные дроби обыкновенных несократимых дробей со знаменателем 61.

4.Используя таблицы индексов, найти остаток от деления числа 27^{29} на число 89.

5. Используя соответствующий признак делимости, проверить делимость чисел 52434, 79974 и 111888 на число 27.

6. С помощью таблиц индексов найти показатель, которому принадлежит число 12 по модулю 59.

7. С помощью таблиц индексов решить сравнение $26x^2 \equiv 67 (\mathrm{mod}\ 73)$.

8. Найти наименьший первообразный корень по модулю 79.

Вариант 10

1. С помощью числа 9 проверить результат арифметических действий
13250100:4569=2800.

2. Найти длину периода и количество цифр между запятой и периодом десятичной дроби, в которую обращается обыкновенная несократимая дробь со знаменателем 760.

3. Используя понятие числа, принадлежащего показателю, найти длину периода при обращении в десятичные дроби обыкновенных несократимых дробей со знаменателем 71.

4. Используя таблицы индексов, найти остаток от деления числа 25^{31} на число 83.

5. Используя соответствующий признак делимости, проверить делимость чисел 3038035 и 3539635 на число 65.

6. С помощью таблиц индексов найти показатель, которому принадлежит число 14 по модулю 59.

7. С помощью таблиц индексов решить сравнение $13x^{11} \equiv 8 (\mathrm{mod}\ 61)$.

8. Найти наименьший первообразный корень по модулю 53.

ВОПРОСЫ К ЗАЧЕТУ
II ЧАСТЬ

1. Сформулировать и доказать свойства сравнений.
2. Полная система вычетов по данному модулю.
3.Приведенная система вычетов по данному модулю.
4.Теорема Эйлера и теорема Ферма.
5. Метод Эйлера для решения сравнений первой степени.
6. Метод подходящих дробей для решения сравнений первой степени.
7 . Китайская теорема об остатках.
8. Сравнения по простому модулю с одним неизвестным (теоремы о числе решений).
9. Теорема Вильсона.
10.Квадратичные вычеты и невычеты по данному модулю. Критерий Эйлера.
11. Символ Лежандра и его свойства.
12. Показатель числа по данному модулю.
13. Первообразные корни по простому модулю.
14. Индексы и их свойства.
15. Признаки делимости.
16. Длина периода десятичной дроби.

ПРИЛОЖЕНИЕ

ТАБЛИЦА ИНДЕКСОВ

Простое число 3

N	0	1	2	3	4	5	6	7	8	9
0		0	1							

I	0	1	2	3	4	5	6	7	8	9
0	1	2								

Простое число 5

N	0	1	2	3	4	5	6	7	8	9
0		0	1	3	2					

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	3						

Простое число 7

N	0	1	2	3	4	5	6	7	8	9
0		0	2	1	4	5	3			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	2	6	4	5				

Простое число 11

N	0	1	2	3	4	5	6	7	8	9
0		0	1	8	2	4	9	7	3	6
1	5									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	5	10	9	7	3	6
1										

Простое число 13

N	0	1	2	3	4	5	6	7	8	9
0		0	1	4	2	9	5	11	3	8
1	10	7	6							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	3	6	12	11	9	5
1	10	7								

Простое число 17

N	0	1	2	3	4	5	6	7	8	9
0		0	14	1	12	5	15	11	10	2
1	3	7	13	4	9	6	8			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	10	13	5	15	11	16	14
1	8	7	4	12	2	6				

Простое число 19

N	0	1	2	3	4	5	6	7	8	9
0		0	1	13	2	16	14	6	3	8
1	17	12	15	5	7	11	4	10	9	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	13	7	14	9	18
1	17	15	11	3	6	12	5	10		

Простое число 23

N	0	1	2	3	4	5	6	7	8	9
0		0	2	16	4	1	18	19	6	10
1	3	9	20	14	21	17	8	7	12	15
2	5	13	11							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	2	10	4	20	8	17	16	11
1	9	22	18	21	13	19	3	15	6	7
2	12	14								

Простое число 29

N	0	1	2	3	4	5	6	7	8	9
0		0	1	5	2	22	6	12	3	10
1	23	25	7	18	13	27	4	21	11	9
2	24	17	26	20	8	16	19	15	14	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	3	6	12	24	19
1	9	18	7	14	28	27	25	21	13	26
2	23	17	5	10	20	11	22	15		

Простое число 31

N	0	1	2	3	4	5	6	7	8	9
0		0	24	1	18	20	25	28	12	2
1	14	23	19	11	22	21	6	7	26	4
2	8	29	17	27	13	10	5	3	16	9
3	15									

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	19	26	16	17	20	29
1	25	13	8	24	10	30	28	22	4	12
2	5	15	14	11	2	6	18	23	7	21

Простое число 37

N	0	1	2	3	4	5	6	7	8	9
0		0	1	26	2	23	27	32	3	16
1	24	30	28	11	33	13	4	7	17	35
2	25	22	31	15	29	10	12	6	34	21
3	14	9	5	20	8	19	18			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	27	17	34	31
1	25	13	26	15	30	23	9	18	36	35
2	33	29	21	5	10	20	3	6	12	24
3	11	22	7	14	28	19				

Простое число 41

N	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

I	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7

Простое число 43

N	0	1	2	3	4	5	6	7	8	9
0		0	27	1	12	25	28	35	39	2
1	10	30	13	32	20	26	24	38	29	19
2	37	36	15	16	40	8	17	3	5	41
3	11	34	9	31	23	18	14	7	4	33
4	22	6	21							

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	38	28	41	37	25	32
1	10	30	4	12	36	22	23	26	35	19
2	14	42	40	34	16	5	15	2	6	18
3	11	33	13	39	31	7	21	20	17	8
4	24	29								

Простое число 47

N	0	1	2	3	4	5	6	7	8	9
0		0	18	20	36	1	38	32	8	40
1	19	7	10	11	4	21	26	16	12	45
2	37	6	25	5	28	2	29	14	22	35
3	39	3	44	27	34	33	30	42	17	31
4	9	15	24	13	43	41	23			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	31	14	23	21	11	8	40
1	12	13	18	43	27	41	17	38	2	10
2	3	15	28	46	42	22	16	33	24	26
3	36	39	7	35	34	29	4	20	6	30
4	9	45	37	44	32	19				

Простое число 53

N	0	1	2	3	4	5	6	7	8	9
0		0	1	17	2	47	18	14	3	34
1	48	6	19	24	15	12	4	10	35	37

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	11	22	44	35
1	17	34	15	30	7	14	28	3	6	12

2	49	31	7	39	20	42	25	51	16	46
3	13	33	5	23	11	9	36	30	38	41
4	50	45	32	22	8	29	40	44	21	28
5	43	27	26							

2	24	48	43	33	13	26	52	51	49	45
3	37	21	42	31	9	18	36	19	38	23
4	46	39	25	50	47	41	29	5	10	20
5	40	27								

Простое число 59

N	0	1	2	3	4	5	6	7	8	9
0		0	1	50	2	6	51	18	3	42
1	7	25	52	45	19	56	4	40	43	38
2	8	10	26	15	53	12	46	34	20	28
3	57	49	5	17	41	24	44	55	39	37
4	9	14	11	33	27	48	16	23	54	36
5	13	32	47	22	35	31	21	30	29	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	5	10	20	40
1	21	42	25	50	41	23	46	33	7	14
2	28	56	53	47	35	11	22	44	29	58
3	57	55	51	43	27	54	49	39	19	38
4	17	34	9	18	36	13	26	52	45	31
5	3	6	12	24	48	37	15	30		

Простое число 61

N	0	1	2	3	4	5	6	7	8	9
0		0	1	6	2	22	7	49	3	12
1	23	15	8	40	50	28	4	47	13	26
2	24	55	16	57	9	44	41	18	51	35
3	29	59	5	21	48	11	14	39	27	46
4	25	54	56	43	17	34	58	20	10	38
5	45	53	42	33	19	37	52	32	36	31
6	30									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	3	6	12	24
1	48	35	9	18	36	11	22	44	27	54
2	47	33	5	10	20	40	19	38	15	30
3	60	59	57	53	45	29	58	55	49	37
4	13	26	52	43	25	50	39	17	34	7
5	14	28	56	51	41	21	42	23	46	31
6										

Простое число 67

N	0	1	2	3	4	5	6	7	8	9
0		0	1	39	2	15	40	23	3	12
1	16	59	41	19	24	54	4	64	13	10
2	17	62	60	28	42	30	20	51	25	44
3	55	47	5	32	65	38	14	22	11	58
4	18	53	63	9	61	27	29	50	43	46
5	31	37	21	57	52	8	26	49	45	36
6	56	7	48	35	6	34	33			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	61	55	43
1	19	38	9	18	36	5	10	20	40	13
2	26	52	37	7	14	28	56	45	23	46
3	25	50	33	66	65	63	59	51	35	3
4	6	12	24	48	29	58	49	31	62	57
5	47	27	54	41	15	30	60	53	39	11
6	22	44	21	42	17	34				

Простое число 71

N	0	1	2	3	4	5	6	7	8	9
0		0	6	26	12	28	32	1	18	52
1	34	31	38	39	7	54	24	49	58	16
2	40	27	37	15	44	56	45	8	13	68
3	60	11	30	57	55	29	64	20	22	65
4	46	25	33	48	43	10	21	9	50	2
5	62	5	51	23	14	59	19	42	4	3
6	66	69	17	53	36	67	63	47	61	41
7	35									

I	0	1	2	3	4	5	6	7	8	9
0	1	7	49	59	58	51	2	14	27	47
1	45	31	4	28	54	23	19	62	8	56
2	37	46	38	53	16	41	3	21	5	35
3	32	11	6	42	10	70	64	22	12	13
4	20	69	57	44	24	26	40	67	43	17
5	48	52	9	63	15	34	25	33	18	55
6	30	68	50	66	36	39	60	65	29	61
7										

Простое число 73

N	0	1	2	3	4	5	6	7	8	9
0		0	8	6	16	1	14	33	24	12
1	9	55	22	59	41	7	32	21	20	62
2	17	39	63	46	30	2	67	18	49	35
3	15	11	40	61	29	34	28	64	70	65
4	25	4	47	51	71	13	54	31	38	66
5	10	27	3	53	26	56	57	68	43	5
6	23	58	19	45	48	60	69	50	37	52
7	42	44	36							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	52	41	59	3	15	2	10
1	50	31	9	45	6	30	4	20	27	62
2	18	17	12	60	8	40	54	51	36	34
3	24	47	16	7	35	29	72	68	48	21
4	32	14	70	58	71	63	23	42	64	28
5	67	43	69	53	46	11	55	56	61	13
6	65	33	19	22	37	39	49	26	57	66
7	38	44								

Простое число 79

N	0	1	2	3	4	5	6	7	8	9
0		0	4	1	8	62	5	53	12	2
1	66	68	9	34	57	63	16	21	6	32
2	70	54	72	26	13	46	38	3	61	11
3	67	56	20	69	25	37	10	19	36	35
4	74	75	58	49	76	64	30	59	17	28
5	50	22	42	77	7	52	65	33	15	31
6	71	45	60	55	24	18	73	48	29	27
7	41	51	14	44	23	47	40	43	39	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	2	6	18	54	4	12
1	36	29	8	24	72	58	16	48	65	37
2	32	17	51	74	64	34	23	69	49	68
3	46	59	19	57	13	39	38	35	26	78
4	76	70	52	77	73	61	25	75	67	43
5	50	71	55	7	21	63	31	14	42	47
6	62	28	5	15	45	56	10	30	11	33
7	20	60	22	66	40	41	44	53		

Простое число 83

N	0	1	2	3	4	5	6	7	8	9
0		0	1	72	2	27	73	8	3	62
1	28	24	74	77	9	17	4	56	63	47
2	29	80	25	60	75	54	78	52	10	12
3	18	38	5	14	57	35	64	20	48	67
4	30	40	81	71	26	7	61	23	76	16
5	55	46	79	59	53	51	11	37	13	34
6	19	66	39	70	6	22	15	45	58	50
7	36	33	65	69	21	44	49	32	68	43
8	31	42	41							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	45	7	14
1	28	56	29	58	33	66	49	15	30	60
2	37	74	65	47	11	22	44	5	10	20
3	40	80	77	71	59	35	70	57	31	62
4	41	82	81	79	75	67	51	19	38	76
5	69	55	27	54	25	50	17	34	68	53
6	23	46	9	19	36	72	61	39	78	73
7	63	43	3	6	12	24	48	13	26	52
8	21	42								

Простое число 89

N	0	1	2	3	4	5	6	7	8	9
0		0	16	1	32	70	17	81	48	2
1	86	84	33	23	9	71	64	6	18	35
2	14	82	12	57	49	52	39	3	25	59
3	87	31	80	85	22	63	34	11	51	24

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	81	65	17	51	64	14
1	42	37	22	66	20	60	2	6	18	54
2	73	41	34	13	39	28	84	74	44	43
3	40	31	4	12	36	19	57	82	68	26

4	30	21	10	29	28	72	73	54	65	74
5	68	7	55	78	19	66	41	36	75	43
6	15	69	47	83	8	5	13	56	38	58
7	79	62	50	20	27	53	67	77	40	42
8	46	4	37	61	26	76	45	60	44	

4	78	56	79	59	88	86	80	62	8	24
5	72	38	25	75	47	52	67	23	69	29
6	87	83	71	35	16	48	55	76	50	61
7	5	15	45	46	49	58	85	77	53	70
8	32	7	21	63	11	33	10	30		

Простое число 97

N	0	1	2	3	4	5	6	7	8	9
0		0	34	70	66	1	8	31	6	44
1	35	86	42	25	65	71	40	89	78	81
2	69	5	24	77	76	2	59	18	3	13
3	9	46	74	60	27	32	16	91	19	95
4	7	85	39	4	58	45	15	84	14	62
5	36	63	93	10	52	87	37	55	47	67
6	43	64	80	75	12	26	94	57	61	51
7	66	11	50	28	29	72	53	21	33	30
8	41	88	23	17	73	90	38	83	92	54
9	79	56	49	20	22	82	48			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	28	43	21	8	40	6	30
1	53	71	64	29	48	46	36	83	27	38
2	93	77	94	82	22	13	65	34	73	74
3	79	7	35	78	2	10	50	56	86	42
4	16	80	12	60	9	45	31	58	96	92
5	72	69	54	76	89	57	91	67	44	26
6	33	68	49	51	61	14	70	59	4	20
7	3	15	75	84	32	63	24	23	18	90
8	62	19	95	87	47	41	11	55	81	17
9	85	37	88	52	66	39				

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Александров В.А., Горшенин С.М.* Задачник – практикум по теории чисел. М.: Учпедгиз, 1972.
2. *Бухштаб А.А.* Теория чисел. М.: Учпедгиз, 1960.
3. *Виноградов И.М.* Основы теории чисел. М.: Наука,1995.
4. *Гайнов А.Т.* Теория чисел. Изд - во НГУ, 1995.
5. *Галочкин А.И., Нестеренко Н.В., Шидловский А.Б.* Введение в теорию чисел. Изд - во МГУ, 1995.
6. *Грибанов В.У., Титов Л.И.* Сборник упражнений по теории чисел. М.: Просвещение, 1964.
7. *Кудреватов Г.А.* Сборник задач по теории чисел. М.: Просвещение, 1970.
8. *Ляпин С.Е., Баранова И.В., Борчугова З.Г.* Сборник задач по элементарной математике. М.: Просвещение, 1973.
9. *Окунев Л.Я.* Краткий курс теории чисел. М.: Учпедгиз, 1956.
10. *Пензин Ю.Г., Клейменов В.Ф.* Сравнения. Учебно-методические разработки (тексты лекций). Изд-во ИГУ, 1998.
11. *Серр Ж*. Курс арифметики. М.: Мир, 1972.

СОДЕРЖАНИЕ

Наталья Владимировна Кван,
старший преподаватель кафедры МАиМ АмГУ

Практикум по теории чисел. Часть II.
Учебно - методическое пособие.

Изд - во АмГУ. Подписано к печати 0.0.03. Формат 60х84/16.Усл. печ. л. , уч. – изд. л. 2,25. тираж 100. Заказ .