

Федеральное агентство по образованию
Государственное образовательное учреждение
высшего профессионального образования
"Удмуртский государственный университет"

Т.М. Банникова, Н.А. Баранова

Теория чисел

Ижевск 2007

УДК
ББК

Банникова Т.М., Баранова Н.А.

Учебно-методическое пособие по теории чисел
Ижевск, 2007. 57 с.

Данное пособие предназначено для студентов математического факультета и факультета информационных технологий и вычислительной техники.. Пособие может быть использовано при организации лабораторных и самостоятельных работ студентов по курсам «Алгебра», «Геометрия и алгебра», «Алгебра и геометрия», а так же пособие может быть полезно студентам математического факультета, изучающим спецкурс «Теоретико-числовые основы криптографии».

© Банникова Т.М., Н.А. Баранова, 2007
© ГОУ ВПО «Удмуртский государственный университет», 2007

Лабораторная работа №1.

**Делимость целых чисел, Н.О.Д., Н.О.К. и их свойства.
Подходящие дроби.**

Вариант 0.

1. Найдите каноническое разложение числа $m=2420$.
2. Найдите наименьшее общее кратное (НОК) чисел $[2,5,8]$.
3. Найдите все простые числа из промежутка $[800; 830]$, используя «решето Эратосфена».
4. Найти наибольший общий делитель (НОД) чисел и его линейное представление (с проверкой):
а) $(733, 1998)$; б) $(2, 5, 8)$.
5. Докажите свойство: если для целых чисел a и b существуют целые x и y такие, что $ax+by=1$, то $\text{НОД}(a, b)=1$.
6. Решите Диофантово уравнение при помощи линейного представления НОД и проверьте два частных решения:
 $47x-111y=89$.
7. Представьте число $\lambda=\frac{153}{38}$ в виде непрерывной дроби, используя алгоритм Евклида.
8. Найдите шестую подходящую дробь для числа $\lambda=\frac{5391}{3976}$.
9. Решите Диофантово уравнение при помощи подходящих дробей: $47x-111y=89$.

Вариант 1.

1. Найдите каноническое разложение числа $m=2880$.
2. Найдите наименьшее общее кратное (НОК) чисел $[7, 15, 18]$.
3. Найдите все простые числа из промежутка $[810; 840]$, используя «решето Эратосфена».
4. Найдите наибольший общий делитель (НОД) чисел и его линейное представление (с проверкой):
а) $(739, 1999)$; б) $(7, 15, 18)$.
5. Докажите свойство: если $\text{НОД}(a, b)=1$, то $\text{НОД}(ac, b)=\text{НОД}(c, b)$ для любого целого c .
6. Решите Диофантово уравнение при помощи линейного представления НОД и проверьте два частных решения:
 $43x - 111y = 87$.
7. Представьте число $\lambda = \frac{105}{33}$ в виде непрерывной дроби, используя алгоритм Евклида.
8. Найдите шестую подходящую дробь для числа $\lambda = \frac{5391}{3977}$.
9. Решите Диофантово уравнение при помощи подходящих дробей: $43x - 111y = 87$.

Вариант 2.

1. Найдите каноническое разложение числа $m=3380$.
2. Найдите наименьшее общее кратное (НОК) чисел $[3,10,15]$.
3. Найдите все простые числа из промежутка $[820; 850]$, используя «решето Эратосфена».
4. Найти наибольший общий делитель (НОД) чисел и его линейное представление (с проверкой):
а) $(743,2000)$; б) $(3, 10, 15)$.
5. Докажите свойство: если $\text{НОД}(a, b)=d$, то $\text{НОД}(a/d, b/d)=1$.
6. Решите Диофантово уравнение при помощи линейного представления НОД и проверьте два частных решения:
 $41x-111y=87$.
7. Представьте число $\lambda=\frac{105}{31}$ в виде непрерывной дроби, используя алгоритм Евклида.
8. Найдите шестую подходящую дробь для числа $\lambda=\frac{5391}{3995}$.
9. Решите Диофантово уравнение при помощи подходящих дробей: $41x-111y=87$.

Вариант 3.

1. Найдите каноническое разложение числа $m=3920$.
2. Найдите наименьшее общее кратное (НОК) чисел $[3,8,19]$.
3. Найдите все простые числа из промежутка $[830; 860]$, используя «решето Эратосфена».
4. Найти наибольший общий делитель (НОД) чисел и его линейное представление (с проверкой):
а) $(751, 2001)$; б) $(3, 8, 19)$.
5. Докажите свойство: если $\text{НОД}(a, b)=1$, $\text{НОД}(c, b)=1$, то $\text{НОД}(ac, b)=1$.
6. Решите Диофантово уравнение при помощи линейного представления НОД и проверьте два частных решения:
 $39x-111y=89$.
7. Представьте число $\lambda=\frac{105}{29}$ в виде непрерывной дроби, используя алгоритм Евклида.
8. Найдите шестую подходящую дробь для числа $\lambda=\frac{5391}{3971}$.
9. Решите Диофантово уравнение при помощи подходящих дробей: $39x-111y=89$.

Вариант 4.

1. Найдите каноническое разложение числа $m=5780$.
2. Найдите наименьшее общее кратное (НОК) чисел $[3,2,26]$.
3. Найдите все простые числа из промежутка $[840; 870]$, используя «решето Эратосфена».
4. Найти наибольший общий делитель (НОД) чисел и его линейное представление (с проверкой):
а) $(757, 2002)$; б) $(3, 2, 26)$.
5. Докажите свойство: если $\text{НОД}(a, b)=d$, то найдутся такие целые числа x и y , что $ax+by=d$.
6. Решите Диофантово уравнение при помощи линейного представления НОД и проверьте два частных решения: $35x-111y=89$.
7. Представьте число $\lambda=\frac{105}{32}$ в виде непрерывной дроби, используя алгоритм Евклида.
8. Найдите шестую подходящую дробь для числа $\lambda=\frac{5391}{3887}$.
9. Решите Диофантово уравнение при помощи подходящих дробей: $35x-111y=89$.

Вариант 5.

1. Найдите каноническое разложение числа $m=6480$.
2. Найдите наименьшее общее кратное (НОК) чисел $[2, 15, 18]$.
3. Найдите все простые числа из промежутка $[850; 880]$, используя «решето Эратосфена».
4. Найти наибольший общий делитель (НОД) чисел и его линейное представление (с проверкой):
а) $(761, 2003)$; б) $(2, 15, 18)$.
5. Докажите свойство: $\text{НОД}(am, bm) = m \cdot \text{НОД}(a, b)$ для любого целого m .
6. Решите Диофантово уравнение при помощи линейного представления НОД и проверьте два частных решения: $44x - 111y = 89$.
7. Представьте число $\lambda = \frac{105}{34}$ в виде непрерывной дроби, используя алгоритм Евклида.
8. Найдите шестую подходящую дробь для числа $\lambda = \frac{5391}{3983}$.
9. Решите Диофантово уравнение при помощи подходящих дробей: $44x - 111y = 89$.

Вариант 6.

1. Найдите каноническое разложение числа $m=7220$.
2. Найдите наименьшее общее кратное (НОК) чисел $[2, 10, 15]$.
3. Найдите все простые числа из промежутка $[860; 890]$, используя «решето Эратосфена».
4. Найти наибольший общий делитель (НОД) чисел и его линейное представление (с проверкой):
а) $(769, 2004)$; б) $(2, 10, 15)$.
5. Докажите свойство: если $\text{НОД}(a, c)=1$, $a|(bc)$, то $a|b$.
6. Решите Диофантово уравнение при помощи линейного представления НОД и проверьте два частных решения: $38x-111y=89$.
7. Представьте число $\lambda=\frac{105}{36}$ в виде непрерывной дроби, используя алгоритм Евклида.
8. Найдите шестую подходящую дробь для числа $\lambda=\frac{5391}{3979}$.
9. Решите Диофантово уравнение при помощи подходящих дробей: $38x-111y=89$.

Вариант 7.

1. Найдите каноническое разложение числа $m=8820$.
2. Найдите наименьшее общее кратное (НОК) чисел $[7,10,15]$.
3. Найдите все простые числа из промежутка $[870; 900]$, используя «решето Эратосфена».
4. Найти наибольший общий делитель (НОД) чисел и его линейное представление (с проверкой):
а) $(773, 2005)$; б) $(7, 10, 15)$.
5. Докажите свойство: если $a|b$, $c|d$, то $(ac)|(bd)$.
6. Решите Диофантово уравнение при помощи линейного представления НОД и проверьте два частных решения: $40x-111y=89$.
7. Представьте число $\lambda=\frac{105}{39}$ в виде непрерывной дроби, используя алгоритм Евклида.
8. Найдите шестую подходящую дробь для числа $\lambda=\frac{5391}{3982}$.
9. Решите Диофантово уравнение при помощи подходящих дробей: $40x-111y=89$.

Вариант 8.

1. Найдите каноническое разложение числа $m=4410$.
2. Найдите наименьшее общее кратное (НОК) чисел $[7, 2, 26]$.
3. Найдите все простые числа из промежутка $[880; 910]$, используя «решето Эратосфена».
4. Найти наибольший общий делитель (НОД) чисел и его линейное представление (с проверкой):
а) $(787, 2006)$; б) $(7, 2, 26)$.
5. Докажите свойство: если $a|(bc)$, $\text{НОД}(a, c)=1$, то $a|b$.
6. Решите Диофантово уравнение при помощи линейного представления НОД и проверьте два частных решения: $46x-111y=89$.
7. Представьте число $\lambda=\frac{105}{41}$ в виде непрерывной дроби, используя алгоритм Евклида.
8. Найдите шестую подходящую дробь для числа $\lambda=\frac{5391}{3985}$.
9. Решите Диофантово уравнение при помощи подходящих дробей: $46x-111y=89$.

Вариант 9.

1. Найдите каноническое разложение числа $m=5290$.
2. Найдите наименьшее общее кратное (НОК) чисел $[7,35,8]$.
3. Найдите все простые числа из промежутка $[890; 920]$, используя «решето Эратосфена».
4. Найти наибольший общий делитель (НОД) чисел и его линейное представление (с проверкой):
а) $(797, 2007)$; б) $(7, 35, 8)$.
5. Докажите свойство: если $a|b$, $c|b$ и $\text{НОД}(a, c)=1$, то $(ac)|b$.
6. Решите Диофантово уравнение при помощи линейного представления НОД и проверьте два частных решения: $49x-111y=89$.
7. Представьте число $\lambda=\frac{105}{41}$ в виде непрерывной дроби, используя алгоритм Евклида.
8. Найдите шестую подходящую дробь для числа $\lambda=\frac{5391}{3988}$.
9. Решите Диофантово уравнение при помощи подходящих дробей: $49x-111y=89$.

Вариант 10.

1. Найдите каноническое разложение числа $m=5394$.
2. Найдите наименьшее общее кратное (НОК) чисел $[7, 15, 8]$.
1. Найдите все простые числа из промежутка $[900; 930]$, используя «решето Эратосфена».
4. Найти наибольший общий делитель (НОД) чисел и его линейное представление (с проверкой):
а) $(751; 2008)$; б) $(7, 15, 8)$.
5. Докажите свойство: если $a|b$ и $a|c$, то $a|\text{НОД}(b, c)$.
6. Решите Диофантово уравнение при помощи линейного представления НОД и проверьте два частных решения:
 $34x - 111y = 89$.
7. Представьте число $\lambda = \frac{105}{43}$ в виде непрерывной дроби, используя алгоритм Евклида.
8. Найдите шестую подходящую дробь для числа $\lambda = \frac{5391}{3986}$.
9. Решите Диофантово уравнение при помощи подходящих дробей: $34x - 111y = 89$.

Решение 0 варианта.

1. Найдите каноническое разложение числа $m=2420$.

Решение:

$$m=2420=2 \cdot 1210=2 \cdot 2 \cdot 605=2 \cdot 2 \cdot 5 \cdot 121=2 \cdot 2 \cdot 5 \cdot 11 \cdot 11.$$

$$\text{Ответ: } m=2^2 \cdot 5 \cdot 11^2.$$

2. Найдите наименьшее общее кратное (НОК) чисел $[2, 5, 8]$.

Решение: НОК - есть наименьшее натуральное число, делящееся на все числа из заданного набора.

Так как 8 уже делится на 2, то НОК $[2, 5, 8]=5 \cdot 8=40$.

$$\text{Ответ: } \text{НОК } [2, 5, 8]=40.$$

3. Найдите все простые числа из промежутка $[800; 830]$, используя «решето Эратосфена».

Решение: найдем простые проверочные числа: $\sqrt{830} < 29$. По решету Эратосфена вычеркнем последовательно все числа делящиеся на 2, 3, 5, 7, 11, 13, 17, 19, 23 из заданного промежутка:

800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815
816 817 818 819 820 821 822 823 824 825 826 827 828 829 830.

(На 2 делятся: 800, 802...каждое второе;

на 3 делятся: 801, 804...каждое третье;

на 5 делятся: 800, 805...каждое пятое;

на 7 делятся: 805, 812...каждое седьмое;

на 11 делятся: 803, 814...каждое одиннадцатое;

на 13 делятся: 806, 819...каждое тринадцатое;

и т.д.

$$\text{Ответ: } 809, 811, 821, 823.$$

4. Найти наибольший общий делитель (НОД) чисел и его линейное представление: а) (733, 1998); б) (2, 5, 8).

а). Решение: НОД - есть наибольшее натуральное число, делящее нацело любое число из заданного набора. Известно, что

один из способов нахождения НОД двух (а следовательно и любого количества) чисел есть – алгоритм Евклида: последний, отличный от нуля, остаток в алгоритме Евклида есть НОД (a, b).

Итак решение нашей следующей задачи основывается на алгоритме Евклида:

$$1998=733\cdot 2+532$$

$$733=532\cdot 1+201$$

$$532=201\cdot 2+130$$

$$201=130\cdot 1+71$$

$$130=71\cdot 1+59$$

$$71=59\cdot 1+12$$

$$59=12\cdot 4+11$$

$$12=11\cdot 1+1$$

$$11=1\cdot 11+0$$

Поэтому по указанному выше НОД (1998, 733)=1.

Из данного алгоритма можно получить линейное представление НОД (1998, 733), рассматривая алгоритм "с конца".

Линейное представление:

$$\begin{aligned} 1 &= 12-11 = 12-(59-12\cdot 4) = 12\cdot 5-59 = (71-59)\cdot 5-59 = 71\cdot 5-6\cdot 59 = \\ &= 5\cdot 71-6\cdot (130-71)=11\cdot 71-6\cdot 130=11\cdot (201-130)-6\cdot 130 = \\ &= 11\cdot 201-17\cdot 130 = 11\cdot 201-17\cdot (532-201\cdot 2)= \\ &= 45\cdot 201 - 17\cdot 532 = 45\cdot (733-532) - 17\cdot 532 = 45\cdot 733 - 62\cdot 532 = \\ &= 45\cdot 733-62\cdot (1998 - 733\cdot 2) = 169\cdot 733-62\cdot 1998. \end{aligned}$$

$$\text{Проверка: } 169\cdot 733-62\cdot 1998 = 123877 - 123876 = 1.$$

б) Решение: чтобы найти НОД нескольких чисел, несложно понять, что достаточно найти НОД двух чисел, потом НОД полученного НОД и следующего числа и т.д.

То есть, если НОД (b, c)=d, то НОД (a, b, c)=НОД (a, d).

$$\text{НОД}(2, 5, 8)=\text{НОД}(2, \text{НОД}(5, 8))=\text{НОД}(2, 1)=1.$$

Линейное представление в общем случае можно найти так: если НОД (b, c)=d=x•b+y•c, НОД (a, d)=z•a+t•d, то НОД (a, b, c)=z•a+t•(x•b+y•c).

Или подберем ответ сами, что в данном случае совсем не сложно и можно сделать гораздо быстрее, чем искать представление в общем виде, как в п.а): $1=8-5-2$.

Ответ: а) н.о.д.(733, 1198)=1, $1=169\cdot 733-62\cdot 1998$;

б) н.о.д.(2, 5, 8)=1, $1=8-5-2$.

5. Докажите свойство: если для целых чисел a и b существуют целые x и y такие, что $ax+by=1$, то НОД (a , b)=1.

Доказательство: пусть н.о.д.(a , b)= d , тогда $d|a$, $d|b$, значит $a=a^*\cdot d$, $b=b^*\cdot d$, где a^* , b^* - целые числа.

По условию задачи $ax+by=1$, для некоторых x , y . Следовательно, получаем равенство $(a^*\cdot d)x+(b^*\cdot d)y=1$ или $d(a^*\cdot x+b^*\cdot y)=1$.

Значит, по определению делимости целых чисел, число d делит 1.

Но $d>0$, следовательно, $d=1$, то есть н.о.д.(a , b)=1. Ч.т.д.

6. Решите Диофантово уравнение при помощи линейного представления НОД: $47x-111y=89$.

Решение: если н.о.д.(a , b)=1, то найдутся такие x , y , что $a\cdot x+b\cdot y=1$.

Тогда выполнится: $ax\cdot c+by\cdot c=c$.

Н.о.д.(47, 111)=1. Найдем x , y :

$$111=47\cdot 2+17$$

$$47=17\cdot 2+13$$

$$17=13\cdot 1+4$$

$$13=4\cdot 3+1$$

$$4=1\cdot 4+0.$$

Линейное представление:

$$\begin{aligned} 1 &= 13-4\cdot 3=13-(17-13\cdot 1)\cdot 3=13\cdot 4-17\cdot 3=(47-17\cdot 2)\cdot 4-17\cdot 3= \\ &= 47\cdot 4-17\cdot 11=47\cdot 4-(111-47\cdot 2)\cdot 11=47\cdot 26-111\cdot 11. \end{aligned}$$

Тогда выполняется: $89=47\cdot (89\cdot 26)-111\cdot (89\cdot 11)$.

$$x=89\cdot 26+111t;$$

$$y=89\cdot 11+47t, \text{ где } t\text{-любое целое.}$$

Ответ: $x=2314+111t$, $y=979+47t$, $t=\mathbb{Z}$.

7. Представьте число $\lambda = \frac{105}{38}$ в виде непрерывной дроби.

Решение: имеем дробь $\lambda = \frac{105}{38}$. Составим алгоритм

Евклида для (105, 38):

$$105 = 38 \cdot 2 + 29$$

$$38 = 29 \cdot 1 + 9$$

$$29 = 9 \cdot 3 + 2$$

$$9 = 2 \cdot 4 + 1$$

$$2 = 1 \cdot 2 + 0.$$

Тогда $q_1=2$, $q_2=1$, $q_3=3$, $q_4=4$, $q_5=2$.

Ответ: $\lambda = 2 + \frac{1}{1 + \frac{1}{3 + \frac{1}{4 + \frac{1}{2}}}}$.

8. Найдите шестую подходящую дробь для числа

$$\lambda = \frac{5391}{3976}.$$

Решение: известны рекуррентные соотношения: $P_s = q_s \cdot P_{s-1} + P_{s-2}$, $Q_s = q_s \cdot Q_{s-1} + Q_{s-2}$.

Где $P_0=1$, $P_1=q_1$, $Q_0=0$, $Q_1=1$.

Находим q_s по алгоритму Евклида:

$$5391 = 3976 \cdot 1 + 1415$$

$$3976 = 1415 \cdot 2 + 1146$$

$$1415 = 1146 \cdot 1 + 269$$

$$1146 = 269 \cdot 4 + 70$$

$$269 = 70 \cdot 3 + 59$$

$$70 = 59 \cdot 1 + 11$$

Т.е.

$q_1=1$, $q_2=2$, $q_3=1$, $q_4=4$, $q_5=3$, $q_6=1$.

$P_1=1$, $Q_1=1$, $P_2=2 \cdot 1 + 1=3$, $Q_2=2 \cdot 1 + 0=2$, $P_3=1 \cdot 3 + 1=4$, $Q_3=1 \cdot 2 + 1=3$,
 $P_4=4 \cdot 3 + 1=19$,

$$Q_4=4 \cdot 3+2=14, P_5=3 \cdot 19+4=61, Q_5=3 \cdot 14+3=45, P_6=1 \cdot 61+19=80, \\ Q_6=1 \cdot 45+14=59.$$

Ответ: $\delta_6 = \frac{80}{59}.$

9. Решите Диофантово уравнение при помощи подходящих дробей: $47x-111y=89.$

Решение: если НОД $(a, b)=1$, то Диофантово уравнение $by-ax=c$ имеет решение:

$$y=\pm c \cdot Q_{n-1}+b \cdot t,$$

$$x=\pm c \cdot P_{n-1}+a \cdot t,$$

где P_{n-1}/Q_{n-1} предпоследняя подходящая дробь к a/b , t -любое целое, а знак

определяет n : если n -четно, то “-“, иначе “+”.

Из 6 задания имеем: $q_1=2, q_2=2, q_3=1, q_4=3, q_5=4, n=5.$

Тогда $P_0=1, Q_0=0, P_1=2,$

$$Q_1=1, P_2=2 \cdot 2+1=5, Q_2=2 \cdot 1+0=2, P_3=1 \cdot 5+2=7, Q_3=1 \cdot 2+1=3, \\ P_4=3 \cdot 7+5=26,$$

$$Q_4=3 \cdot 3+2=11. \text{ Тогда}$$

$$y=89 \cdot 11+47 \cdot t=979+47t,$$

$$x=89 \cdot 26+111 \cdot t=2314+111t, \text{ где } t\text{-любое целое.}$$

Ответ: $x=2314+111t, y=979+47t, t=\mathbb{Z}.$

Лабораторная работа № 2.

**Сравнения и их свойства.
Решение сравнений первой степени.**

Вариант 0.

1. Найдите значение функции Эйлера для числа $m=2304$.
2. Найти остаток от деления 2^{1037} на 19.
3. Решить сравнение по определению:

$$\text{a) } 8x \equiv 11 \pmod{14}; \quad \text{b) } 3x \equiv 5 \pmod{7}.$$

4. Решить сравнение, используя линейное представление НОД: $3x \equiv 5 \pmod{7}$.
5. Решить сравнение, используя теорему Эйлера:
 $3x \equiv 5 \pmod{7}$.
6. Решить сравнение, используя подходящие дроби:
 $11x \equiv -192 \pmod{401}$.
7. Решить сравнение (случай не единственности решения): $8x \equiv 12 \pmod{14}$.
8. Решить систему сравнений:

$$\text{a) } \begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 8 \pmod{11} \end{cases}; \quad \text{b) } \begin{cases} 4x \equiv 3 \pmod{15} \\ 3x \equiv 1 \pmod{10} \end{cases}$$

9. Докажите, что число вида $3m+2$ (при целом m) не является полным квадратом.

10. Решите систему сравнений с двумя переменными:

$$\begin{cases} 3x + 4y \equiv 29 \pmod{143} \\ 2x - 9y \equiv -84 \pmod{143} \end{cases}$$

Вариант 1.

1. Найдите значение функции Эйлера для числа $m=1152$.

2. Найти остаток от деления 2^{1050} на 17.

3. Решить сравнение по определению:

$$\text{a) } 6x \equiv 11 \pmod{16}; \quad \text{b) } 2x \equiv 3 \pmod{5}.$$

4. Решить сравнение, используя линейное представление НОД: $2x \equiv 3 \pmod{5}$.

5. Решить сравнение, используя теорему Эйлера:
 $2x \equiv 3 \pmod{5}$.

6. Решить сравнение, используя подходящие дроби:
 $3x \equiv -151 \pmod{907}$.

7. Решить сравнение (случай не единственности решения): $6x \equiv 12 \pmod{16}$.

8. Решить систему сравнений:

$$\text{a) } \begin{cases} x \equiv 7 \pmod{11} \\ x \equiv 3 \pmod{63} \end{cases}; \quad \text{b) } \begin{cases} 4x \equiv 6 \pmod{21} \\ 3x \equiv 6 \pmod{14} \end{cases}$$

9. Решите в натуральных числах уравнение $x^2 - y^2 = 31$.

10. Решите систему сравнений с двумя переменными:

$$\begin{cases} 3x + 9y \equiv -3 \pmod{12} \\ 2x + 2y \equiv 10 \pmod{12} \end{cases}$$

Вариант 2.

1. Найдите значение функции Эйлера для числа $m=3456$.

2. Найти остаток от деления 5^{1995} на 9.

3. Решить сравнение по определению:

$$\text{a) } 12x \equiv 17 \pmod{21}; \text{ b) } 17x \equiv 7 \pmod{19}.$$

4. Решить сравнение, используя линейное представление НОД: $17x \equiv 7 \pmod{19}$.

5. Решить сравнение, используя теорему Эйлера: $17x \equiv 7 \pmod{19}$.

6. Решить сравнение, используя подходящие дроби: $3x \equiv -193 \pmod{401}$.

7. Решить сравнение (случай не единственности решения): $12x \equiv 18 \pmod{21}$.

8. Решить систему сравнений:

$$\text{a) } \begin{cases} x \equiv 3 \pmod{7} \\ x \equiv 5 \pmod{6} \end{cases}; \quad \text{b) } \begin{cases} 3x \equiv 1 \pmod{8} \\ 5x \equiv 2 \pmod{14} \end{cases}.$$

9. Докажите, что число вида $5m+2$ (при целом m) не является полным квадратом.

10. Решите систему сравнений с двумя переменными:

$$\begin{cases} x + 2y \equiv 2 \pmod{3} \\ 2x + y \equiv 1 \pmod{3} \end{cases}$$

Вариант 3.

1. Найдите значение функции Эйлера для числа $m=2880$.
2. Найти остаток от деления 7^{1018} на 19.
3. Решить сравнение по определению:

$$\text{a) } 9x \equiv 17 \pmod{24}; \quad \text{b) } 4x \equiv 3 \pmod{7}.$$

4. Решить сравнение, используя линейное представление НОД: $4x \equiv 3 \pmod{7}$.
5. Решить сравнение, используя теорему Эйлера: $4x \equiv 3 \pmod{7}$.
6. Решить сравнение, используя подходящие дроби: $5x \equiv -193 \pmod{401}$.
7. Решить сравнение (случай не единственности решения): $9x \equiv 18 \pmod{24}$.
8. Решить систему сравнений:

$$\text{a) } \begin{cases} x \equiv 7 \pmod{19} \\ x \equiv 2 \pmod{5} \end{cases}; \quad \text{b) } \begin{cases} 2x \equiv 1 \pmod{15} \\ 3x \equiv 1 \pmod{10} \end{cases}.$$

9. Решите в натуральных числах уравнение $x^2 - y^2 = 303$.

10. Решите систему сравнений с двумя переменными:

$$\begin{cases} 5x - y \equiv 3 \pmod{6} \\ 2x + 2y \equiv -1 \pmod{6} \end{cases}$$

Вариант 4.

1. Найдите значение функции Эйлера для числа $m=1440$.
2. Найти остаток от деления 7^{1039} на 13.
3. Решить сравнение по определению:

$$\text{a) } 6x \equiv 11 \pmod{14}; \quad \text{b) } 5x \equiv 4 \pmod{6}.$$

4. Решить сравнение, используя линейное представление НОД: $5x \equiv 4 \pmod{6}$.
5. Решить сравнение, используя теорему Эйлера: $5x \equiv 4 \pmod{6}$.
6. Решить сравнение, используя подходящие дроби: $5x \equiv -192 \pmod{907}$.
7. Решить сравнение (случай не единственности решения): $6x \equiv 10 \pmod{14}$.
8. Решить систему сравнений:

$$\text{a) } \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{2} \end{cases}; \quad \text{b) } \begin{cases} 3x \equiv 2 \pmod{35} \\ 2x \equiv 5 \pmod{21} \end{cases}$$

9. Каково наименьшее натуральное n , такое, что $n!$ делится на 990?

10. Решите систему сравнений с двумя переменными:

$$\begin{cases} x + 2y \equiv 4 \pmod{5} \\ 3x + y \equiv 2 \pmod{5} \end{cases}.$$

Вариант 5.

1. Найдите значение функции Эйлера для числа $m=2880$.

2. Найти остаток от деления 6^{1087} на 11.

3. Решить сравнение по определению:

$$\text{a) } 4x \equiv 5 \pmod{10}; \quad \text{b) } 3x \equiv 2 \pmod{7}.$$

4. Решить сравнение, используя линейное представление НОД: $3x \equiv 2 \pmod{7}$.

5. Решить сравнение, используя теорему Эйлера:
 $3x \equiv 2 \pmod{7}$.

6. Решить сравнение, используя подходящие дроби:
 $7x \equiv -151 \pmod{907}$.

7. Решить сравнение (случай не единственности решения): $4x \equiv 6 \pmod{10}$.

8. Решить систему сравнений:

$$\text{a) } \begin{cases} x \equiv 5 \pmod{7} \\ x \equiv 3 \pmod{5} \end{cases}; \quad \text{b) } \begin{cases} 2x \equiv 1 \pmod{15} \\ 4x \equiv 1 \pmod{21} \end{cases}.$$

9. Натуральные числа x, y, z таковы, что $x^2 + y^2 = z^2$.
Докажите, что хотя бы одно из этих чисел делится на 3.

10. Решите систему сравнений с двумя переменными:

$$\begin{cases} x + 3y \equiv 2 \pmod{5} \\ 4x + y \equiv 2 \pmod{5} \end{cases}.$$

Вариант 6.

1. Найдите значение функции Эйлера для числа $m=3380$.

2. Найти остаток от деления 5^{1105} на 17.

3. Решить сравнение по определению:

$$\text{a) } 6x \equiv 5 \pmod{18}; \quad \text{b) } 2x \equiv 3 \pmod{11}.$$

4. Решить сравнение, используя линейное представление НОД: $2x \equiv 3 \pmod{11}$.

5. Решить сравнение, используя теорему Эйлера:
 $2x \equiv 3 \pmod{11}$.

6. Решить сравнение, используя подходящие дроби:
 $7x \equiv -151 \pmod{401}$.

7. Решить сравнение (случай не единственности решения): $6x \equiv 6 \pmod{18}$.

8. Решить систему сравнений:

$$\text{a) } \begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 1 \pmod{2} \end{cases}; \quad \text{b) } \begin{cases} 2x \equiv 5 \pmod{9} \\ 5x \equiv 1 \pmod{12} \end{cases}.$$

9. Докажите, что ни одно из чисел вида 10^{3n+1} нельзя представить в виде суммы двух кубов натуральных чисел.
10. Решите систему сравнений с двумя переменными:
- $$\begin{cases} x + 2y \equiv 0 \pmod{5} \\ 3x + 2y \equiv 2 \pmod{5} \end{cases}$$

Вариант 7.

1. Найдите значение функции Эйлера для числа $m=3920$.
2. Найти остаток от деления 5^{1712} на 13.
3. Решить сравнение по определению:
$$\text{a) } 9x \equiv 14 \pmod{21}; \quad \text{b) } 3x \equiv 7 \pmod{11}.$$
4. Решить сравнение, используя линейное представление НОД: $3x \equiv 7 \pmod{11}$.
5. Решить сравнение, используя теорему Эйлера:
 $3x \equiv 7 \pmod{11}$.
6. Решить сравнение, используя подходящие дроби:
 $11x \equiv -192 \pmod{907}$.
7. Решить сравнение (случай не единственности решения): $9x \equiv 15 \pmod{21}$.
8. Решить систему сравнений:

$$\text{a) } \begin{cases} x \equiv 7 \pmod{11} \\ x \equiv 3 \pmod{7} \end{cases}; \quad \text{b) } \begin{cases} 4x \equiv 2 \pmod{9} \\ 5x \equiv 1 \pmod{12} \end{cases}.$$

9. Докажите, что число, имеющее нечетное число делителей, есть точный квадрат.

10. Решите систему сравнений с двумя переменными:

$$\begin{cases} x + 3y \equiv 5 \pmod{7} \\ 4x \equiv 5 \pmod{7} \end{cases}.$$

Вариант 8.

1. Найдите значение функции Эйлера для числа $m=5780$.

2. Найти остаток от деления 6^{1079} на 11.

3. Решить сравнение по определению:

$$\text{a) } 6x \equiv 8 \pmod{15}; \quad \text{b) } 4x \equiv 3 \pmod{5}.$$

4. Решить сравнение, используя линейное представление НОД: $4x \equiv 3 \pmod{5}$.

5. Решить сравнение, используя теорему Эйлера: $4x \equiv 3 \pmod{5}$.

6. Решить сравнение, используя подходящие дроби: $3x \equiv -151 \pmod{401}$.

7. Решить сравнение (случай не единственности решения): $6x \equiv 9 \pmod{15}$.

8. Решить систему сравнений:

$$\text{a) } \begin{cases} x \equiv 2 \pmod{7} \\ x \equiv 3 \pmod{5} \end{cases}; \quad \text{b) } \begin{cases} 2x \equiv 14 \pmod{15} \\ 5x \equiv 1 \pmod{21} \end{cases}.$$

9. Может ли $n!$ оканчиваться ровно на 5 нулей?

10. Решите систему сравнений с двумя переменными:

$$\begin{cases} x + 3y \equiv 3 \pmod{5} \\ 3x + 2y \equiv 2 \pmod{5} \end{cases}.$$

Вариант 9.

1. Найдите значение функции Эйлера для числа $m=6480$.

2. Найти остаток от деления 9^{1045} на 11.

3. Решить сравнение по определению:

$$\text{a) } 9x \equiv 8 \pmod{27}; \quad \text{b) } 5x \equiv 2 \pmod{6}.$$

4. Решить сравнение, используя линейное представление НОД: $5x \equiv 2 \pmod{6}$.

5. Решить сравнение, используя теорему Эйлера: $5x \equiv 2 \pmod{6}$.

6. Решить сравнение, используя подходящие дроби: $5x \equiv -151 \pmod{907}$.

7. Решить сравнение (случай не единственности решения): $9x \equiv 9 \pmod{27}$.

8. Решить систему сравнений:

$$\text{a) } \begin{cases} x \equiv 2 \pmod{9} \\ x \equiv 5 \pmod{11} \end{cases}; \quad \text{b) } \begin{cases} 4x \equiv 3 \pmod{25} \\ 7x \equiv 1 \pmod{10} \end{cases}.$$

9. Докажите, что число вида $11m+1$ (при целом m) не является полным квадратом.
10. Решите систему сравнений с двумя переменными:
- $$\begin{cases} 9x + 3y \equiv -3 \pmod{12} \\ 2x + 2y \equiv 10 \pmod{12} \end{cases}.$$

Вариант 10.

1. Найдите значение функции Эйлера для числа $m=7220$.
2. Найти остаток от деления 3^{1072} на 17.
3. Решить сравнение по определению:

$$\text{a) } 4x \equiv 5 \pmod{14}; \quad \text{b) } 5x \equiv 4 \pmod{9}.$$
4. Решить сравнение, используя линейное представление НОД: $5x \equiv 4 \pmod{9}$.
5. Решить сравнение, используя теорему Эйлера:
6. $5x \equiv 4 \pmod{9}$.
7. Решить сравнение, используя подходящие дроби:

$$7x \equiv -192 \pmod{401}.$$
8. Решить сравнение (случай не единственности решения): $4x \equiv 6 \pmod{14}$.

9. Решить систему сравнений:

$$\text{a) } \begin{cases} x \equiv 6 \pmod{7} \\ x \equiv 2 \pmod{5} \end{cases}; \quad \text{b) } \begin{cases} 4x \equiv 1 \pmod{10} \\ 3x \equiv 5 \pmod{8} \end{cases}.$$

10. Докажите, что при условии $56 \cdot a = 65 \cdot b$ число $a+b$ – составное.

11. Решите систему сравнений с двумя переменными:

$$\begin{cases} 3x + 5y \equiv 2 \pmod{7} \\ 4x \equiv 1 \pmod{7} \end{cases}.$$

Решение 0 варианта.

1. Найдите значение функции Эйлера для числа $m=2304$.

Решение: в решении используем свойства функции Эйлера:

- 1). $\varphi(a, b) = \varphi(a) \cdot \varphi(b)$, для тех a, b , что $\text{НОД}(a, b) = 1$;
- 2) $\varphi(p^n) = p^n - p^{n-1}$, для любого простого p .

Найдем каноническое представление числа 2304.

$$2304 = 2 \cdot 1152 = 2 \cdot 2 \cdot 576 = 2 \cdot 2 \cdot 2 \cdot 288 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 144 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 12 \cdot 12 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 4 \cdot 3 = 2^8 \cdot 3^2.$$

$$\text{Тогда } \varphi(2304) = \varphi(2^8) \cdot \varphi(3^2) = (2^8 - 2^7) \cdot (3^2 - 3^1) = 2^7 \cdot 6 = 768.$$

Ответ: $\varphi(2304) = 768$.

2. Найти остаток от деления 2^{1037} на 19.

Решение: при нахождении остатка от деления 2^{1037} на 19, воспользуемся теоремой Ферма:

если для двух натуральных чисел $\text{НОД}(a, b) = 1$, тогда выполняется сравнение:

$$b^{\varphi(a)} \equiv 1 \pmod{a}, \text{ где } \varphi(a) - \text{функция Эйлера.}$$

Так как $\text{НОД}(2, 19)=1$, то $2^{\varphi(19)} \equiv 1 \pmod{19}$, $2^{18} \equiv 1 \pmod{19}$.
 $1037 \equiv 11 \pmod{18}$, то $1037 = 18 \cdot k + 11$, где k - целое число.
 Имеем $2^{1037} \equiv 2^{18 \cdot k + 11} \pmod{19} \equiv 2^{18 \cdot k} \cdot 2^{11} \pmod{19} \equiv$
 $(2^{18})^k \cdot 2^{11} \pmod{19} \equiv 1^k \cdot 2^{11} \pmod{19} \equiv 2048 \pmod{19} \equiv 15 \pmod{19}$.

Ответ: остаток равен 15.

3. Решить сравнение по определению: а) $8x \equiv 11 \pmod{14}$;
 б) $3x \equiv 5 \pmod{7}$.

а) Решение: напомним определение сравнения: пусть число m целое, больше 1, говорят, что целые числа a и b сравнимы друг с другом по модулю m , если $m \mid (a-b)$ и обозначают $a \equiv b \pmod{m}$.

У нас задано $8x \equiv 11 \pmod{14}$. По определению сравнения получаем $14 \mid (8x-11)$, но $(8x-11)$ число нечетное при любом x . Значит, 14 не может делить $(8x-11)$.

Следовательно, сравнение не разрешимо.

б) Решение: задано $3x \equiv 5 \pmod{7}$.

По определению имеем: $7 \mid (3x-5)$, т.е. $3x-5=7k$,
 $x=(5+7k)/3=1+2k+(2+k)/3$.

x – целое число, значит $(2+k)$ должно делиться на 3.

Возьмем в качестве $k=1$, тогда $x=(5+7)/3=4$.

По теореме: сравнение $a \cdot x \equiv 1 \pmod{m}$ разрешимо $\Leftrightarrow \text{НОД}(a, m)=1$, если сравнение разрешимо, то оно имеет единственное решение по модулю m .

$\text{НОД}(3, 7)=1$, то система имеет единственное решение по модулю 7.

Ответ: а) решения нет; б) $x \equiv 4 \pmod{7}$.

4. Решить сравнение, используя линейное представление НОД: $3x \equiv 5 \pmod{7}$.

Решение: задано $3x \equiv 5 \pmod{7}$.

$\text{НОД}(3, 7)=1$, то система имеет единственное решение по модулю 7.

Найдем линейное представление $\text{НОД}(3, 7)=1$.

$$7=3\cdot 2+1;$$

$$3=1\cdot 3;$$

Линейное представление НОД:

$$1=7+3\cdot(-2), \text{ тогда } 3\cdot(-2)\equiv 1 \pmod{7},$$

умножая на 5 обе части сравнения, получаем $3\cdot(-2\cdot 5)\equiv 5 \pmod{7}$
следовательно, $x\equiv -2\cdot 5 \pmod{7} \equiv -10 \pmod{7} \equiv 4 \pmod{7}$.

Ответ: $x\equiv 4 \pmod{7}$.

5. Решить сравнение, используя теорему Эйлера: $3x\equiv 5 \pmod{7}$.

Решение: НОД (3, 7)=1, то система имеет единственное решение по модулю 7.

Вспомним теорему Эйлера: если НОД (a, m)=1, то сравнение $a\cdot x\equiv b \pmod{m}$ разрешимо и имеет единственное решение $x\equiv a^{\varphi(m)-1}\cdot b \pmod{m}$.

Для нашего сравнения имеем: НОД (3, 7)=1, значит, теорема выполняется

$$x\equiv 3^{\varphi(7)-1}\cdot 5 \pmod{7}, x\equiv 3^{6-1}\cdot 5 \pmod{7} \equiv 3^5\cdot 5 \pmod{7},$$

$$x\equiv 9\cdot 9\cdot 3\cdot 5 \pmod{7} \equiv 2\cdot 2\cdot 3\cdot 5 \pmod{7} \equiv 12\cdot 5 \pmod{7},$$

$$x\equiv 5\cdot 5 \pmod{7} \equiv 25 \pmod{7} \equiv 4 \pmod{7}.$$

Ответ: $x\equiv 4 \pmod{7}$.

6. Решить сравнение, используя подходящие дроби: $11x\equiv -192 \pmod{401}$.

Решение: имеем формулу: если $ax\equiv b \pmod{m}$, то $x\equiv (-1)^{n-1}\cdot P_{n-1}\cdot b \pmod{m}$, где $m/a=P_n/Q_n$ – n-ая подходящая дробь. Найдем необходимые P, Q.

$$401=11\cdot 36+5;$$

$$11=5\cdot 2+1;$$

$$5=1\cdot 5.$$

$$\text{Значит } n=3, q_1=36, q_2=2, q_3=5; P_0=1, P_1=36, P_2=2\cdot 36+1=73.$$

$$\text{Тогда } x\equiv (-1)^2\cdot 73\cdot (-192) \pmod{401} \equiv -382 \pmod{401} \equiv 19 \pmod{401}.$$

Ответ: $x\equiv 19 \pmod{401}$.

7. Решить сравнение (случай не единственности решения): $8x \equiv 12 \pmod{14}$.

Решение: $8x \equiv 12 \pmod{14}$, по свойствам сравнений можно разделить все три части сравнения на число 2. Получим $4x \equiv 6 \pmod{7}$. Упростим сравнение: $2x \equiv 3 \pmod{7}$.

Решим любым способом (например, подбором):
 $x \equiv 5 \pmod{7}$.

Так как $\text{НОД}(2, 7)=1$, то решение единственно по $\text{mod } 7$.

Теперь найдем решение по модулю 14: положим $x=5+7t$, где t -целое число, тогда при $t=0$ $x_1 \equiv 5 \pmod{14}$, при $t=1$ $x_2 \equiv 5+7 \pmod{14} \equiv 12 \pmod{14}$.

При больших t получаем $5+7t > 14$, т.е. решения повторяются.

Ответ: $x_1 \equiv 5 \pmod{14}$, $x_2 \equiv 12 \pmod{14}$.

8. Решить систему сравнений:

$$\text{a) } \begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 8 \pmod{11} \end{cases}; \quad \text{b) } \begin{cases} 4x \equiv 3 \pmod{15} \\ 3x \equiv 1 \pmod{10} \end{cases}.$$

а) Решение: рассмотрим систему $\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 8 \pmod{11} \end{cases}$.

Модули обладают свойством $\text{НОД}(5, 11)=1$, то решить систему можно по китайской теореме об остатках. Для этого найдем линейное представление $\text{НОД}(5, 11)$: $1=5 \cdot (-2)+11 \cdot 1$.

Тогда по известным формулам имеем

$$x = 2 \cdot (11 \cdot 1) + 8 \cdot (5 \cdot (-2)).$$

Или $x = 22 - 80 = -58$; $x \equiv -58 \pmod{55} \equiv 52 \pmod{55}$.

б) Решение: $\begin{cases} 4x \equiv 3 \pmod{15} \\ 3x \equiv 1 \pmod{10} \end{cases}$.

Решим независимо каждое сравнение любым способом:

$$\begin{cases} x \equiv 12 \pmod{15} \\ x \equiv 7 \pmod{10} \end{cases}.$$

Так как модули не взаимно простые, то решение находим по модулю $\text{НОК}[10, 15]=30$.

Из первого сравнения получаем $x=12+15\cdot k$, подставим во второе сравнение системы $12+15\cdot k\equiv 7 \pmod{10}$; упростим $15\cdot k\equiv -5 \pmod{10}$; $3k\equiv -1 \pmod{2}$; $k\equiv 1 \pmod{2}$, тогда $k=1+2n$, где n - целое число, подставим k в формулу для x :

$$x=12+15\cdot(1+2n)=27+30n\equiv 27 \pmod{30}.$$

Ответ: а) $x\equiv 52 \pmod{55}$; б) $x\equiv 27 \pmod{30}$.

9. Докажите, что число вида $3m+2$ (при целом m) не является полным квадратом.

Доказательство: доказательство проведем от противного.

Пусть $3m+2=n^2$, при некотором натуральном n .

Рассмотрим остатки от деления n на 3:

$n\equiv 0 \pmod{3}$, или $n\equiv 1 \pmod{3}$, или $n\equiv 2 \pmod{3}$.

Тогда, соответственно, $n^2\equiv 0 \pmod{3}$, или $n^2\equiv 1 \pmod{3}$, или $n^2\equiv 4 \pmod{3}\equiv 1 \pmod{3}$.

Но по условию $n^2=3m+2\equiv 2 \pmod{3}$ – противоречие.

10. Решите систему сравнений с двумя переменными:

$$\begin{cases} 3x + 4y \equiv 29 \pmod{143} \\ 2x - 9y \equiv -84 \pmod{143} \end{cases}.$$

Решение основывается на свойствах сравнений. Обратим внимание на то, что число 143- простое.

Умножим первое сравнение на 9, а второе на 4 и сложим их. Умножим первое сравнение на 2, а второе на -3 и сложим их. Получим систему сравнений с двумя

переменными:
$$\begin{cases} 35x \equiv -75 \pmod{143} \\ 35y \equiv 310 \pmod{143} \end{cases}.$$

Решаем каждое сравнение по отдельности:

$$\begin{cases} 7x \equiv -15 \pmod{143} \\ 35y \equiv 310 \pmod{143} \end{cases} \quad \begin{cases} x \equiv 100 \pmod{143} \\ y \equiv 111 \pmod{143} \end{cases}$$

Ответ: $x\equiv 100 \pmod{143}$, $y\equiv 111 \pmod{143}$.

Лабораторная работа №3.

Сравнения высших степеней. Символ Якоби.

Вариант 0.

1. Покажите, что для любого целого $n \equiv 1 \pmod{2}$ выполняется: $n^{12} - n^8 - n^4 + 1 \equiv 0 \pmod{512}$.
2. Найдите группу Z_{10}^* обратимых элементов кольца Z_{10} и все ее подгруппы. Указать цикличность группы. Найти все образующие.
3. Найдите все примитивные корни по модулю $m=25$.
4. Найдите сравнение степени ниже p , равносильное данному:
 $3x^{14} + 4x^{13} + 3x^{12} + 2x^{11} + x^9 + 2x^8 + 4x^7 + x^6 + 3x^4 + x^3 + 4x^2 + 2x \equiv 0 \pmod{5}$, если $p=5$.
5. Найдите сравнение со старшим коэффициентом равным 1, равносильное данному: $3x^4 + 2x^3 + 3x^2 + 2x \equiv 0 \pmod{5}$.
6. Решите сравнение $f(x) \equiv 0 \pmod{27}$, используя решение сравнение $f(x) \equiv 0 \pmod{3}$, если $f(x) = x^4 + 7x + 4$.
7. Решите сравнение по составному модулю:
 $32x^5 + 57x^3 + 96x + 191 \equiv 0 \pmod{6}$.
8. Найдите число решений сравнения:
а) $x^2 \equiv -2 \pmod{209}$; б) $x^6 \equiv 1 \pmod{37}$.
9. Решите сравнение второй степени:
а) $x^2 \equiv -1 \pmod{10}$; б) $x^2 \equiv -1 \pmod{25}$.

10. Вычислите символ Якоби:

$$\text{a) } \left(\frac{3592}{5471} \right). \text{ b) } \left(\frac{1031}{1297} \right).$$

11. Найдите систему индексов числа a по модулю m , если $a=13$, $m=20$.

Вариант 1.

1. Докажите, что последняя цифра квадрата числа равна 6, если число его десятков нечетно.
2. Найдите группу Z_{11}^* обратимых элементов кольца Z_{11} и все ее подгруппы. Указать цикличность группы. Найти все образующие.
3. Найдите все примитивные корни по модулю $m=50$.
4. Найдите сравнение степени ниже p , равносильное данному: $x^{16}+x^4+x^2+1 \equiv 0 \pmod{5}$, если $p=5$.
5. Найдите сравнение со старшим коэффициентом равным 1, равносильное данному: $3x^3-2x^2+x-1 \equiv 0 \pmod{7}$.
6. Решите сравнение $f(x) \equiv 0 \pmod{27}$, используя решение сравнения $f(x) \equiv 0 \pmod{3}$, если $f(x)=x^3-6x^2+11x-6$.
7. Решите сравнение по составному модулю: $x^4-x^3+2x+1 \equiv 0 \pmod{30}$.
8. Найдите число решений сравнения:
a) $x^2 \equiv 1 \pmod{16}$; b) $x^6 \equiv 1 \pmod{19}$.
9. Решите сравнение второй степени:
a) $x^2 \equiv 13 \pmod{34}$; b) $x^2 \equiv 13 \pmod{289}$.

10. Вычислите символ Якоби:

$$\text{a) } \left(\frac{2621}{2887} \right) \quad \text{b) } \left(\frac{911}{467} \right).$$

11. Найдите систему индексов числа a по модулю m , если $a=17$, $m=28$.

Вариант 2.

1. Найдите все числа, для которых $63^n - 5^n \equiv 0 \pmod{1972}$.
2. Найдите группу Z_{12}^* обратимых элементов кольца Z_{12} и все ее подгруппы. Указать цикличность группы. Найти все образующие.
3. Найдите все примитивные корни по модулю $m=100$.
4. Найдите сравнение степени ниже p , равносильное данному: $x^{16} + x^8 + 1 \equiv 0 \pmod{7}$, если $p=7$.
5. Найдите сравнение со старшим коэффициентом равным 1, равносильное данному: $3x^4 - 5x^3 + 4x^2 - 2x + 1 \equiv 0 \pmod{10}$.
6. Решите сравнение $f(x) \equiv 0 \pmod{27}$, используя решение сравнение $f(x) \equiv 0 \pmod{3}$, если $f(x) = x^4 + 4x^3 + 4x$.
7. Решите сравнение по составному модулю: $x^5 - 12x^3 + 36x - 12 \equiv 0 \pmod{30}$.
8. Найдите число решений сравнения:

$$\text{a) } x^2 \equiv 2 \pmod{105}; \quad \text{b) } x^5 \equiv 1 \pmod{19}.$$

9. Решите сравнение второй степени:

a) $x^2 \equiv 2 \pmod{34}$; b) $x^2 \equiv 2 \pmod{289}$.

10. Вычислите символ Якоби:

a) $\left(\frac{907}{2833}\right)$ b) $\left(\frac{4201}{5867}\right)$.

11. Найдите систему индексов числа a по модулю m , если $a=19$, $m=28$.

Вариант 3.

1. Пусть $p > 3$ - простое число и десятичная запись числа p^n состоит из 20 цифр. Покажите, что среди них найдутся, по крайней мере, 3 одинаковые цифры.

2. Найдите группу Z_{13}^* обратимых элементов кольца Z_{13} и все ее подгруппы. Указать цикличность группы. Найти все образующие.

3. Найдите все примитивные корни по модулю $m=27$.

4. Найдите сравнение степени ниже p , равносильное данному: $x^4 - 12x^3 + 47x^2 - 60 \equiv 0 \pmod{3}$, если $p=3$.

5. Найдите сравнение со старшим коэффициентом равным 1, равносильное данному:

$$2x^4 + 3x^3 - 3x^2 - 5x + 2 \equiv 0 \pmod{7}.$$

6. Решите сравнение $f(x) \equiv 0 \pmod{27}$, используя решение сравнения $f(x) \equiv 0 \pmod{3}$, если $f(x) = x^5 + x^4 - 10x^2 + 2$.

7. Решите сравнение по составному модулю:
 $x^4 - 8x^3 + 12x^2 - 6x + 2 \equiv 0 \pmod{30}$.
8. Найдите число решений сравнения:
 а) $x^2 \equiv 3 \pmod{43}$; б) $x^4 \equiv 1 \pmod{29}$.
9. Решите сравнение второй степени:
 а) $x^2 \equiv 8 \pmod{34}$; б) $x^2 \equiv 8 \pmod{289}$.
10. Вычислите символ Якоби:
 а) $\left(\frac{266}{2166}\right)$. б) $\left(\frac{4400}{4409}\right)$.
11. Найдите систему индексов числа a по модулю m , если
 $a=13$, $m=28$.

Вариант 4.

1. Покажите, что число $(2^m - 1)$ – составное, если m – составное.
2. Найдите группу Z_{14}^* обратимых элементов кольца Z_{14} и все ее подгруппы. Указать цикличность группы. Найти все образующие.
3. Найдите все примитивные корни по модулю $m=54$.
4. Найдите сравнение степени ниже p , равносильное данному: $x^5 + x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod{3}$, если $p=3$.
5. Найдите сравнение со старшим коэффициентом равным 1, равносильное данному: $2x^3 + x^2 - x - 1 \equiv 0 \pmod{25}$.

6. Решите сравнение $f(x) \equiv 0 \pmod{64}$, используя решение сравнения $f(x) \equiv 0 \pmod{2}$, если $f(x) = 9x^2 + 29x + 62$.
7. Решите сравнение по составному модулю:
 $x^6 - 6x^5 + 11x^4 - x^3 - 18x^2 + 20x - 8 \equiv 0 \pmod{30}$.
8. Найдите число решений сравнения:
 а) $x^2 \equiv -2 \pmod{143}$; б) $x^7 \equiv 1 \pmod{29}$.
9. Решите сравнение второй степени:
 а) $x^2 \equiv 9 \pmod{52}$; б) $x^2 \equiv 9 \pmod{169}$.
10. Вычислите символ Якоби:
 а) $\left(\frac{1307}{5987}\right)$ б) $\left(\frac{2018}{2213}\right)$.
11. Найдите систему индексов числа a по модулю m , если $a=15$, $m=28$.

Вариант 5.

1. Покажите что, если число $p = 2^m + 1$ – простое, то $m = 2^k$ для некоторого $k \geq 0$ – целого.
2. Найдите группу Z_{15}^* обратимых элементов кольца Z_{15} и все ее подгруппы. Указать цикличность группы. Найти все образующие.
3. Найдите все примитивные корни по модулю $m=22$.
4. Найдите сравнение степени ниже p , равносильное данному: $x^4 - x^3 + x - 1 \equiv 0 \pmod{3}$, если $p=3$.
5. Найдите сравнение со старшим коэффициентом равным 1, равносильное данному: $3x^4 - 4x^3 - x^2 - x - 2 \equiv 0 \pmod{14}$.

6. Решите сравнение $f(x) \equiv 0 \pmod{125}$, используя решение сравнения $f(x) \equiv 0 \pmod{5}$, если $f(x) = x^3 + 2x^2 + 4$.

7. Решите сравнение по составному модулю:
 $x^5 + x^4 - 6x^3 - 14x^2 - 11x - 3 \equiv 0 \pmod{30}$.

8. Найдите число решений сравнения:

$$x^2 \equiv 2 \pmod{19}; \quad \text{b) } x^6 \equiv 1 \pmod{29}.$$

9. Решите сравнение второй степени:

$$\text{a) } x^2 \equiv 10 \pmod{52}; \quad \text{b) } x^2 \equiv 10 \pmod{169}.$$

10. Вычислите символ Якоби:

$$\text{a) } \left(\frac{1741}{2053} \right) \quad \text{b) } \left(\frac{362}{2281} \right).$$

11. Найдите систему индексов числа a по модулю m , если $a=11$, $m=28$.

Вариант 6.

1. Покажите что, если $m \equiv 1 \pmod{2}$, то $(2^m + 1)$ – составное.

2. Найдите группу Z_{16}^* обратимых элементов кольца Z_{16} и все ее подгруппы. Указать цикличность группы. Найти все образующие.

3. Найдите все примитивные корни по модулю $m=26$.

4. Найдите сравнение степени ниже p , равносильное данному: $x^5 - 6x^3 + 2x^2 - 4 \equiv 0 \pmod{3}$, если $p=3$.

5. Найдите сравнение со старшим коэффициентом равным 1, равносильное данному:
 $4x^4 - 2x^3 - 16x^2 + 5x + 9 \equiv 0 \pmod{17}$.
6. Решите сравнение $f(x) \equiv 0 \pmod{625}$, используя решение сравнения $f(x) \equiv 0 \pmod{5}$, если $f(x) = x^4 + 4x^3 + 2x^2 + 2x + 11$.
7. Решите сравнение по составному модулю:
 $x^4 + 4x^3 - 2x^2 - 12x + 9 \equiv 0 \pmod{30}$.
8. Найдите число решений сравнения:
 а) $x^2 \equiv -4 \pmod{221}$; б) $x^6 \equiv 1 \pmod{31}$.
9. Решите сравнение второй степени:
 а) $x^2 \equiv 10 \pmod{26}$; б) $x^2 \equiv 1 \pmod{169}$.
10. Вычислите символ Якоби:
 а) $\left(\frac{82}{709}\right)$ б) $\left(\frac{2837}{5783}\right)$
11. Найдите систему индексов числа a по модулю m , если $a=9$, $m=28$.

Вариант 7.

1. Пусть $a > 0$, $m > 1$ – целые числа. Докажите, что числа $(a^m + 1)$ и $(a^m - 1)$ – составные.
2. Найдите группу Z_{17}^* обратимых элементов кольца Z_{17} и все ее подгруппы. Указать цикличность группы. Найти все образующие.
3. Найдите все примитивные корни по модулю $m=34$.

4. Найдите сравнение степени ниже p , равносильное данному: $x^7 - 1 \equiv 0 \pmod{5}$, если $p=5$.
5. Найдите сравнение со старшим коэффициентом равным 1, равносильное данному: $3x^6 - 3x^4 + 7x^3 - 6x + 2 \equiv 0 \pmod{10}$.
6. Решите сравнение $f(x) \equiv 0 \pmod{27}$, используя решение сравнения $f(x) \equiv 0 \pmod{3}$, если $f(x) = 7x^4 + 19x + 25$.
7. Решите сравнение по составному модулю: $x^4 + 2x^3 - 13x^2 - 38x - 24 \equiv 0 \pmod{30}$.
8. Найдите число решений сравнения:
 а) $x^2 \equiv -2 \pmod{187}$; б) $x^5 \equiv 1 \pmod{31}$.
9. Решите сравнение второй степени:
 а) $x^2 \equiv 1 \pmod{88}$; б) $x^2 \equiv 1 \pmod{121}$.
10. Вычислите символ Якоби:
 а) $\left(\frac{5483}{5939}\right)$ б) $\left(\frac{2026}{3011}\right)$.
11. Найдите систему индексов числа a по модулю m , если $a=5$, $m=28$.

Вариант 8.

1. Докажите, что равенство $11 \dots 11 = a^2$ - невозможно ни при каких целых числах a и n (n - количество 1 в числе).

2. Найдите группу Z_{18}^* обратимых элементов кольца Z_{18} и все ее подгруппы. Указать цикличность группы. Найти все образующие.

3. Найдите все примитивные корни по модулю $m=38$.

4. Найдите сравнение степени ниже p , равносильное данному: $x^6 - 64 \equiv 0 \pmod{5}$, если $p=5$.

5. Найдите сравнение со старшим коэффициентом равным 1, равносильное данному:
 $3x^5 + 8x^4 + 9x^3 + 15x^2 + 10x + 9 \equiv 0 \pmod{17}$.

6. Решите сравнение $f(x) \equiv 0 \pmod{27}$, используя решение сравнения $f(x) \equiv 0 \pmod{3}$, если $f(x) = 7x^4 + x^3 + 19x + 18$.

7. Решите сравнение по составному модулю:
 $x^5 - 2x^4 - 4x^3 + 4x^2 - 5x + 6 \equiv 0 \pmod{30}$.

8. Найдите число решений сравнения:
а) $x^2 \equiv -8 \pmod{187}$; б) $x^3 \equiv 1 \pmod{31}$.

9. Решите сравнение второй степени:
а) $x^2 \equiv 9 \pmod{40}$; б) $x^2 \equiv 9 \pmod{25}$.

10. Вычислите символ Якоби:

$$\text{а) } \left(\frac{1822}{1913} \right) \quad \text{б) } \left(\frac{811}{2797} \right).$$

11. Найдите систему индексов числа a по модулю m , если $a=3$, $m=28$.

Вариант 9.

1. Найти n , при которых $x^{2n}+x+1$ делится на x^2+x+1 .

2. Найдите группу Z_{19}^* обратимых элементов кольца Z_{19} и все ее подгруппы. Указать цикличность группы. Найти все образующие.

3. Найдите все примитивные корни по модулю $m=23$.

4. Найдите сравнение степени ниже p , равносильное данному: $x^5+3x^4+4x^3-2x^2+5x-5 \equiv 0 \pmod{3}$, если $p=3$.

5. Найдите сравнение со старшим коэффициентом равным 1, равносильное данному: $2x^3-x^2-5x+4 \equiv 0 \pmod{7}$.

6. Решите сравнение $f(x) \equiv 0 \pmod{625}$, используя решение сравнение $f(x) \equiv 0 \pmod{5}$, если $f(x)=x^4+9x^3-2x^2+7x+21$.

7. Решите сравнение по составному модулю: $x^5-7x^3-12x^2+6x+36 \equiv 0 \pmod{30}$.

8. Найдите число решений сравнения:

$$\text{a) } x^2 \equiv -1 \pmod{221}; \text{ b) } x^{15} \equiv 1 \pmod{31}.$$

9. Решите сравнение второй степени:

$$\text{a) } x^2 \equiv 1 \pmod{56}; \text{ b) } x^2 \equiv 1 \pmod{49}.$$

10. Вычислите символ Якоби:

$$\text{a) } \left(\frac{222}{1783} \right) \text{ b) } \left(\frac{1103}{1409} \right).$$

11. Найдите систему индексов числа a по модулю m , если $a=31$, $m=28$.

Вариант 10.

1. Покажите, что для любого целого $n \geq 1$ выполняется:
 $n^6 + 2n^5 - n^2 - 2n \equiv 0 \pmod{120}$.

2. Найдите группу Z_{20}^* обратимых элементов кольца Z_{20} и все ее подгруппы. Указать цикличность группы. Найти все образующие.

3. Найдите все примитивные корни по модулю $m=46$.

4. Найдите сравнение степени ниже p , равносильное данному: $x^6 - 4x^4 + x^3 - 2x^2 + 5 \equiv 0 \pmod{5}$, если $p=5$.

5. Найдите сравнение со старшим коэффициентом равным 1, равносильное данному:
 $2x^5 - 9x^4 + 2x^3 + 37x^2 + 10x - 14 \equiv 0 \pmod{7}$.

6. Решите сравнение $f(x) \equiv 0 \pmod{125}$, используя решение сравнения $f(x) \equiv 0 \pmod{5}$, если $f(x) = x^3 + 2x + 5$.

7. Решите сравнение по составному модулю:
 $x^4 - 2x^3 - 8x^2 + 13x - 24 \equiv 0 \pmod{30}$.

8. Найдите число решений сравнения:

$$x^2 \equiv -9 \pmod{221}; \quad \text{b) } x^{10} \equiv 1 \pmod{31}.$$

9. Решите сравнение второй степени:

$$\text{a) } x^2 \equiv 1 \pmod{44}; \quad \text{b) } x^2 \equiv 1 \pmod{121}.$$

10. Вычислите символ Якоби:

$$\text{a) } \left(\frac{1951}{2549} \right) \quad \text{b) } \left(\frac{1092}{1381} \right).$$

11. Найдите систему индексов числа a по модулю m , если $a=33$, $m=28$.

Решение 0 варианта.

1. Покажите, что для любого целого $n \equiv 1 \pmod{2}$ выполняется: $n^{12} - n^8 - n^4 + 1 \equiv 0 \pmod{512}$.

Решение: преобразуем левую часть сравнения

$$\begin{aligned} n^{12} - n^8 - n^4 + 1 &= n^8 \cdot (n^4 - 1) - (n^4 - 1) = (n^8 - 1) \cdot (n^4 - 1) = \\ &= (n^4 - 1) \cdot (n^4 + 1) \cdot (n^2 - 1) \cdot (n^2 + 1) = (n - 1)^2 \cdot (n^4 + 1) \cdot (n^2 + 1)^2 \cdot (n + 1)^2. \end{aligned}$$

По условию задачи $n \equiv 1 \pmod{2}$, или $n = 1 + 2k$, при целом k , тогда:

$$(n - 1)^2 = 4k^2 \equiv 0 \pmod{4}, \quad (n + 1)^2 = 4 \cdot (1 + k)^2 \equiv 0 \pmod{4},$$

$$(n^2 + 1)^2 = 4 \cdot (2k^2 + 2k + 1) \equiv 0 \pmod{4},$$

$$(n^4 + 1) = 2 \cdot (8k^4 + 16k^3 + 12k^2 + 4k + 1) \equiv 0 \pmod{2}.$$

Значит

$$\begin{aligned} n^{12} - n^8 - n^4 + 1 &= 4k^2 \cdot 4(1 + k)^2 \cdot 4(2k^2 + 2k + 1) \cdot \\ &2(8k^4 + 16k^3 + 12k^2 + 4k + 1) \equiv 0 \pmod{2^7}. \end{aligned}$$

При этом если k четное то $k^2 \equiv 0 \pmod{4}$ следовательно, $n^{12} - n^8 - n^4 + 1 \equiv 0 \pmod{2^9} \equiv 0 \pmod{512}$.

Если k нечетно то $(1 + k)^2 \equiv 0 \pmod{4}$ следовательно, $n^{12} - n^8 - n^4 + 1 \equiv 0 \pmod{2^9} \equiv 0 \pmod{512}$.

1. Найдите группу Z_{10}^* обратимых элементов кольца Z_{10} и все ее подгруппы. Указать цикличность группы. Найти все образующие.

Решение: найдем группу $Z_{10}^* = \{1, 3, 7, 9\}$, так как ее элементы взаимно просты с модулем.

При этом $|Z_{10}^*| = \varphi(10) = \varphi(2) \cdot \varphi(5) = 1 \cdot 4 = 4$.

Для определения цикличности и нахождения подгрупп, найдем порядки элементов этой группы:

$|1|=1$, $|3|=4$, так как $3^4 \equiv 1 \pmod{10}$ и $3^n \not\equiv 1 \pmod{10}$ при $n < 4$;

$|7|=4$, так как $7^4 \equiv 1 \pmod{10}$ и $7^n \not\equiv 1 \pmod{10}$ при $n < 4$;

$|9|=2$, так как $9^2 \equiv 1 \pmod{10}$ и $9^n \not\equiv 1 \pmod{10}$ при $n < 2$.

Из выше сказанного получаем только одну подгруппу $H = \langle 9 \rangle$. $|H|=2$.

Образующие данной группы 3 и 7, то есть

$$Z_{10}^* = \langle 3 \rangle = \langle 7 \rangle.$$

Ответ: $Z_{10}^* = \{1, 3, 7, 9\} = \langle 3 \rangle = \langle 7 \rangle$ -циклическая, подгруппа $H = \langle 9 \rangle$.

3. Найдите все примитивные корни по модулю $m=25$.

Решение: по определению, все примитивные корни по модулю $m=25$ таковы, что

$Z_{25}^* = \langle a \rangle$. Это означает, что $0 < a < 25$, $\text{НОД}(a, m) = 1$ и $|a| = \varphi(25) = 25 - 5 = 20$.

Определим порядки всех элементов группы Z_{25}^* , зная, что порядок элемента делит порядок группы равный $\varphi(25) = 20$. Значит, порядки элементов могут быть равны 2, 4, 5, 10 или 20:

$|1|=1$, $|2|=20$, $|3|=20$, $|4|=10$, $|6|=5$, $|7|=4$, $|8|=20$, $|9|=10$, $|11|=5$, $|12|=20$, $|13|=20$, $|14|=10$, $|16|=5$, $|17|=20$, $|18|=4$, $|19|=10$, $|21|=5$, $|22|=20$, $|23|=20$, $|24|=2$.

Ответ: 2, 3, 8, 12, 13, 17, 22, 23.

4. Найдите сравнение степени ниже p , равносильное данному:

$$3x^{14} + 4x^{13} + 3x^{12} + 2x^{11} + x^9 + 2x^8 + 4x^7 + x^6 + 3x^4 + x^3 + 4x^2 + 2x \equiv 0 \pmod{5}, \text{ если } p=5.$$

Решение: $p=5$ - простое, значит по теореме Ферма выполняется: $x^p \equiv x \pmod{p}$,

для $p=5$ $x^5 \equiv x \pmod{5}$, следовательно $x^{14} = x^{10} \cdot x^4 \equiv x^2 \cdot x^4 \pmod{5} \equiv$

$\equiv x^5 \cdot x \pmod{p} \equiv x^2 \pmod{p}$. Аналогично находим:
 $x^{13} \equiv x \pmod{5}$; $x^{12} \equiv x^4 \pmod{5}$; $x^{11} \equiv x^3 \pmod{5}$; $x^{10} \equiv x^2 \pmod{5}$;
 $x^9 \equiv x \pmod{5}$; $x^8 \equiv x^4 \pmod{5}$;
 $x^7 \equiv x^3 \pmod{5}$; $x^6 \equiv x^2 \pmod{5}$.

Тогда

$$\begin{aligned} 3x^{14} + 4x^{13} + 3x^{12} + 2x^{11} + x^9 + 2x^8 + 4x^7 + x^6 + 3x^4 + x^3 + 4x^2 + 2x &\equiv \\ \equiv 3x^2 + 4x + 3x^4 + 2x^3 + x + 2x^4 + 4x^3 + x^2 + 3x^4 + x^3 + 4x^2 + 2x &\equiv \\ 8x^4 + 7x^3 + 8x^2 + 7x \pmod{5} &\equiv \\ \equiv 3x^4 + 2x^3 + 3x^2 + 2x \pmod{5}. \end{aligned}$$

Ответ: $3x^4 + 2x^3 + 3x^2 + 2x \equiv 0 \pmod{5}$.

5. Найдите сравнение со старшим коэффициентом равным 1, равносильное данному:

$$3x^4 + 2x^3 + 3x^2 + 2x \equiv 0 \pmod{5}.$$

Решение: НОД (3, 5) = 1, значит будем искать множитель h такой, чтобы

$$h \cdot (3x^4 + 2x^3 + 3x^2 + 2x) \equiv h \cdot 3x^4 + h \cdot 2x^3 + h \cdot 3x^2 + h \cdot 2x \equiv 0 \pmod{5} \text{ и}$$

при этом $3 \cdot h \equiv 1 \pmod{5}$.

Легко найти $h \equiv 2 \pmod{5}$ – решение сравнения $3 \cdot h \equiv 1 \pmod{5}$.

$$\text{Тогда} \quad h(x) \equiv h \cdot f(x) \equiv 2 \cdot (3x^4 + 2x^3 + 3x^2 + 2x) \equiv x^4 + 4x^3 + x^2 + 4x \pmod{5}.$$

Ответ: $x^4 + 4x^3 + x^2 + 4x \equiv 0 \pmod{5}$.

6. Решите сравнение $f(x) \equiv 0 \pmod{27}$, используя решение сравнение $f(x) \equiv 0 \pmod{3}$, если $f(x) = x^4 + 7x + 4$.

Решение: решим сначала сравнение $x^4 + 7x + 4 \equiv 0 \pmod{3}$.

Имеем: $x^4 + x + 1 \equiv 0 \pmod{3}$, решением является $x \equiv 1 \pmod{3}$.

При этом $f'(x) = 4x^3 + 7$, $f'(1) \not\equiv 0 \pmod{3}$. Значит, по известным формулам, находим x , как $x \equiv 1 + t \cdot 3 \pmod{3^2}$, где t является решением сравнения $f'(1) \cdot t \equiv -f(1)/3 \pmod{3}$:

т.е. $11 \cdot t \equiv -4 \pmod{3}$, подбираем $t \equiv 1 \pmod{3}$.

Подставляем $x \equiv 1 + t \cdot 3 \pmod{3^2} \equiv 1 + 1 \cdot 3 \equiv 4 \pmod{9}$.

По аналогии, находим x в виде $x \equiv 4 + t \cdot 9 \pmod{3^3}$, где t является решением сравнения

$$f'(4) \cdot t \equiv -f(4)/9 \pmod{3}: 263 \cdot t \equiv -32 \pmod{3}, \text{ т.е. } t \equiv 2 \pmod{3}.$$

Подставляем $x \equiv 4 + t \cdot 9 \pmod{3^3} \equiv 4 + 2 \cdot 9 \equiv 22 \pmod{27}$.

Ответ: $x \equiv 22 \pmod{27}$.

7. Решите сравнение по составному модулю:

$$32x^5 + 57x^3 + 96x + 191 \equiv 0 \pmod{6}.$$

Решение: решение сравнения по составному модулю сводится к решению системы

$$\text{сравнений: } \begin{cases} 32x^5 + 57x^3 + 96x + 191 \equiv 0 \pmod{2}, \\ 32x^5 + 57x^3 + 96x + 191 \equiv 0 \pmod{3} \end{cases}$$

$$\begin{cases} x^3 + 1 \equiv 0 \pmod{2}, \\ 2x^5 + 2 \equiv 0 \pmod{3}. \end{cases}$$

Так как Z_2, Z_3 – поля, то каждое сравнение имеет корней не более чем его степень, и каждый корень берется из минимальной системы вычетов. Имеем только по одному

$$\text{решению: } \begin{cases} x \equiv 1 \pmod{2}, \\ x \equiv 2 \pmod{3}. \end{cases}$$

Решаем систему и находим ответ.

Ответ: $x \equiv 5 \pmod{6}$.

8. Найдите число решений сравнения:

$$\text{а) } x^2 \equiv -2 \pmod{209}; \text{ б) } x^6 \equiv 1 \pmod{37}.$$

а). Решение: число решений сравнения $x^2 \equiv a \pmod{m_1 \cdot m_2}$ равно числу решений системы:

$$\begin{cases} x^2 \equiv a \pmod{m_1}, \\ x^2 \equiv a \pmod{m_2}. \end{cases}$$

Число решений сравнения $x^2 \equiv a \pmod{p}$ равно 2, если $a^{p-1/2} \equiv 1 \pmod{p}$.

Имеем

$$\begin{cases} x^2 \equiv -2 \pmod{11}, (-2)^5 \equiv 1 \pmod{11}, \text{ имеет 2 решения} \\ x^2 \equiv -2 \pmod{19}, (-2)^9 \equiv 1 \pmod{19}, \text{ имеет 2 решения.} \end{cases}$$

Система имеет 4 решения.

б). Решение: число решений сравнения $x^n \equiv 1 \pmod{p}$ равно n , если $(p-1)/n$.

В нашем сравнении $p=37$, $n=6$, значит, условие выполняется.

Сравнение $x^6 \equiv 1 \pmod{37}$ имеет 6 решений.

Ответ: а). 4; б) 6.

9. Решите сравнение второй степени:

а) $x^2 \equiv -1 \pmod{10}$; б) $x^2 \equiv -1 \pmod{25}$.

а). Решение: решение либо существует, либо нет.

Проверим условие

$(-1)^{\varphi(10)/d} \equiv 1 \pmod{10}$: $\varphi(10)=4$, $(-1)^2 \equiv 1 \pmod{10}$ - верно значит, решение существует.

НОД $(2, 4)=2=d$ значит, существует ровно 2 решения. Найдем их. $x^2 \equiv -1 \pmod{10}$, $x^2 \equiv 9 \pmod{10}$, следовательно $x \equiv \pm 3 \pmod{10}$.

б). $x^2 \equiv -1 \pmod{25}$. Проверим условие $(-1)^{\varphi(25)/d} \equiv 1 \pmod{25}$: $\varphi(25)=20$, $(-1)^{10} \equiv 1 \pmod{25}$ - верно значит, решение существует. Н.о.д. $(2, 20)=2=d$ значит, существует ровно 2 решения.

Решим сначала сравнение $x^2 \equiv -1 \pmod{5}$, $x^2 \equiv 4 \pmod{5}$, $x \equiv \pm 2 \pmod{5}$.

Тогда $x=2+5t$, $x^2=4+20t+25t^2$, $x^2 \equiv 4+20t \equiv -1 \pmod{25}$, $20t \equiv -5 \pmod{25}$, $4t \equiv -1 \pmod{5}$,

$4t \equiv 4 \pmod{5}$, $t \equiv 1 \pmod{5}$, $x \equiv 2+5 \cdot 1 \pmod{25} \equiv 7 \pmod{25}$.

Тогда второе решение будет $x \equiv -7 \pmod{25} \equiv 18 \pmod{25}$.

Ответ: а) $x_1 \equiv 3 \pmod{10}$, $x_2 \equiv 7 \pmod{10}$;

б) $x_1 \equiv 7 \pmod{25}$, $x_2 \equiv 18 \pmod{25}$.

10. Вычислите символ Якоби:

$$\text{a) } \left(\frac{3592}{5471} \right); \text{ b) } \left(\frac{1031}{1297} \right).$$

а). Решение: решение основывается на свойствах символа Якоби.

Все переходы расписаны по порядку:

$$\begin{aligned} \left(\frac{3592}{5471} \right) &= \left(\frac{8}{5471} \right) \cdot \left(\frac{449}{5471} \right) = \left(\frac{5471}{449} \right) = \left(\frac{83}{449} \right) = \left(\frac{449}{83} \right) = \left(\frac{34}{83} \right) = \\ &= \left(\frac{2}{83} \right) \cdot \left(\frac{17}{83} \right) = - \left(\frac{17}{83} \right) = - \left(\frac{83}{17} \right) = - \left(\frac{15}{17} \right) = - \left(\frac{17}{15} \right) = - \left(\frac{2}{15} \right) \end{aligned}$$

1) Разложим на множители $3592=8 \cdot 449$; $8=2^3$, $5471 \equiv 7 \pmod{8} \equiv -1 \pmod{8}$, тогда $(2/5471)=1$, $(8/5471)=1$.

2) Перевернем символ со знаком + так как $(5471-1)/2=2735$, $(449-1)/2=224$, $(-1)^{2735 \cdot 224}=1$.

3) Упростим $5471 \equiv 83 \pmod{449}$; перевернем символ со знаком + так как $(83-1)/2=41$, $(449-1)/2=224$, $(-1)^{41 \cdot 224}=1$.

4) Упростим $449 \equiv 34 \pmod{83}$, разложим на множители $34=2 \cdot 17$; $83 \equiv 3 \pmod{8}$, значит, $(2/83)=-1$.

5) Перевернем символ со знаком + так как $(83-1)/2=41$, $(17-1)/2=8$, $(-1)^{41 \cdot 8}=1$.

Упростим $83 \equiv 15 \pmod{17}$.

6) Перевернем символ со знаком + так как $(17-1)/2=8$, $(15-1)/2=7$, $(-1)^{8 \cdot 7}=1$.

Упростим $17 \equiv 2 \pmod{15}$.

7) Так как $15 \equiv -1 \pmod{8}$, тогда $(2/15)=1$. Общий результат $=-1$.

б). Решение:

$$\begin{aligned} \left(\frac{1031}{1297} \right) &= \left(\frac{1297}{1031} \right) = \left(\frac{226}{1031} \right) = \left(\frac{2}{1031} \right) \cdot \left(\frac{133}{1031} \right) = \left(\frac{1031}{133} \right) = \\ &= \left(\frac{100}{133} \right) = \left(\frac{2}{133} \right)^2 = \left(\frac{5}{133} \right)^5 \end{aligned}$$

1) Перевернем символ со знаком + так как $(1297-1)/2=648$, $(1031-1)/2=515$, $(-1)^{648 \cdot 515}=1$.
 2) Упростим $1297 \equiv 266 \pmod{1031}$.
 3) Разложим на множители $266=2 \cdot 133$. Символ $(2/1031)=1$, так как $1031 \equiv -1 \pmod{8}$.
 4) Перевернем символ со знаком + так как $(1031-1)/2=515$, $(133-1)/2=66$, $(-1)^{515 \cdot 66}=1$.
 5) Упростим $1031 \equiv 100 \pmod{133}$.
 6) Разложим на множители $100=2^2 \cdot 5^2$, получаем оба символа в квадратах значит, каждый из них равен 1 а значит результат =1.
Ответ: а) -1: б) 1.

11. Найдите систему индексов числа а по модулю m, если $a=13$, $m=20$.

Решение: так как $m=20=2^2 \cdot 5$, то $Z_{20}^* = Z_4^* \times Z_5^* = \langle -1 \rangle \times \langle 3 \rangle$, по условию $a=13$.

Найдем систему индексов из условий $13 \equiv (-1)^x \pmod{4}$, $13 \equiv 3^v \pmod{5}$:
 $x=0$, $v=1$.

Ответ: $\{0, 1\}$.