Министерство науки и высшего образования Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ
ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

Ю.Б. Ржонсницкая, И.В. Зайцева, Е.А. Бровкина

ОСНОВЫ ТЕОРИИ ЧИСЕЛ

Учебное пособие

Санкт-Петербург
РГГМУ
2022

УДК 511(075.8)
ББК 22.13я73
Р48

Одобрено Научно-методическим советом РГГМУ

Рецензент: Петрова В.В. доцент кафедры высшей математики и физики РГГМУ

Ржонсницкая Ю. Б., Зайцева И.В.,Бровкина Е.А

Основы теории чисел. Учебное пособие / Ю.Б. Ржонсницкая, И.В. Зайцева, Е.А. Бровкина. – Санкт-Петербург : РГГМУ, 2022. – 82 с.

ISBN 978-5-86813-571-2

Предлагаемое пособие адресовано преподавателям и студентам и предназначено для проведения практических занятий и самостоятельных работ в аудитории и выдачи ИДЗ.

ISBN 978-5-86813-571-2

Глава 1

Решение задач

1.1 Наибольший общий делитель. Линейное представление НОД

Определение. Наибольшим общим делителем целых чисел a и b (НОД(a, b)), является целое число d , которое удовлетворяет условиям:

1. $d \geq 0$,
2. $a \vdots d$ и $b \vdots d$,
3. если $a \vdots c$ и $b \vdots c$ тогда $d \vdots c$

Теорема 1 (Алгоритм деления)**.** *Даны целые числа a и b, $b \neq 0$. Тогда существует единственная пара целых чисел q (неполное частное) и r (остаток), такие, что $a=bq+r$ и $0 \leq r < |b|$.*

Теорема 2. *Пусть* $a{=}bq{+}r$ *, где* q *– неполное частное и* r *– остаток. Тогда*

НОД$(a, b) =$ *НОД*(b, r).

Алгоритм Евклида Пусть $a > b$.

- $a = bq_1 + r_1, \quad 0 < r_1 < b$
- $b = r_1q_2 + r_2, \quad 0 < r_2 < r_1$
- . . . . . .
- $r_{k-1} = r_kq_{k+1} + r_{k+1} \quad 0 < r_{k+1} < r_k$
- . . . . . .
- $r_{n-2} = r_{n-1}q_{n-1} + r_n, \quad 0 < r_n < r_{n-1}$
- $r_{n-1} = r_nq_{n+1}, \quad (r_{n+1} = 0)$.

Здесь $k = 0, 1, \ldots, n-1, \quad a = r_{-1}, \quad b = r_0$. Тогда НОД($a$,$b$)=$r_n$, где r_n ***–последний ненулевой остаток.***

Теорема 3 (Линейное представление НОД)**.** *Для* a *и* $b \in \mathbb{Z}$ *НОД*$(a, b) = d \Leftrightarrow$ *существуют* x *и* $y \in \mathbb{Z}$*, такие что,*

$$ax + by = d.$$

Задача 2. *Найти наибольший общий делитель (НОД) чисел* $a = 1234$ *и* $b = 4321$ *с помощью алгоритма Евклида. Представить НОД как линейную комбинацию чисел a и b (найти коэффициенты разложения* $d = ax + by$*).*[1]

[1]Полезно продолжить изучение основ по книгам Виноградова И.М. (гл. 1) или Дэвенпорта Г.(гл. 1).

Решение. Для решения первой части задачи применим алгоритм Евклида к числам $a = 1234$ и $b = 4321$. Для работы алгоритма безразлично, в каком порядке используются *a* и *b*, однако для ускорения процесса, лучше взять в качестве первого числа наибольшее, т.е. 4321.

(1) $4321 = 1234 \cdot 3 + 619$; НОД$(4321, 1234) =$ НОД$(1234, 619)$

($b = a \cdot 3 + r_1$)

(Поделили b на a с остатком. Остаток равен 619, неполное частное 3)

(2) $1234 = 619 \cdot 1 + 615$; НОД$(1234, 619) =$ НОД$(619, 615)$

($a = r_1 \cdot 1 + r_2$)

(Остаток равен 615, неполное частное 1)

(3) $619 = 615 \cdot 1 + 4$; НОД$(619, 615) =$ НОД$(615, 4)$

($r_1 = r_2 \cdot 1 + r_3$)

(Продолжаем в том же духе. В данном алгоритме нам понадобятся только остатки, а неполные частные - это полезный побочный продукт, который пригодится нам при решении следующих задач.)

(4) $615 = 4 \cdot 153 + 3$; НОД$(615, 4) =$ НОД$(4, 3)$

($r_2 = r_3 \cdot 153 + r_4$)

(Уже, вобщем-то понятно, что НОД$(4, 3) = 1$, но мы все равно проведем алгоритм до конца из уважения к Евклиду.)

(5) $4 = 3 \cdot 1 + 1$; НОД$(4, 3) =$ НОД$(3, 1)$

($r_3 = r_4 \cdot 1 + r_5$)

(6) $3 = 1 \cdot 3 + 0$; НОД$(3, 1) =$ НОД$(1, 0) = 1$

($r_6 = 0$)

(Неизбежно мы приходим к нулевому остатку и алгоритм завершает свою работу.)

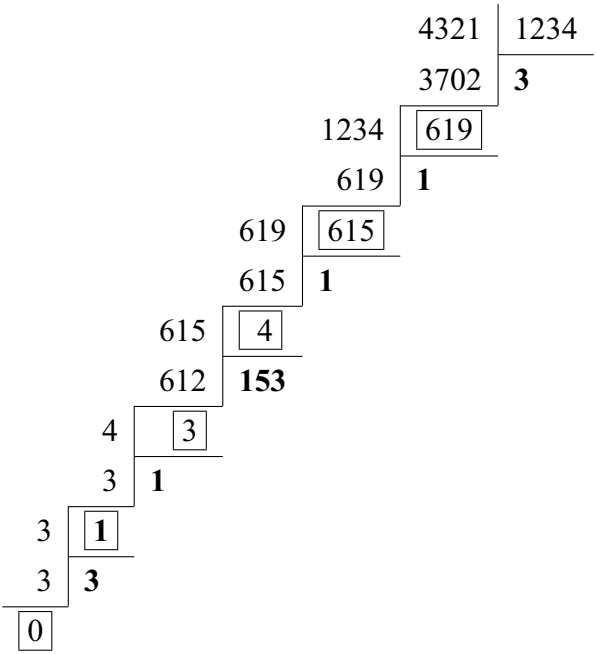
Получили цепочку равенств:

НОД$(4321, 1234)$ = НОД$(1234, 619)$ = ... = НОД $(1, 0) = 1$,

которая и дает нам конечный ответ. Проще говоря, НОД – это *последний ненулевой остаток* в алгоритме Евклида.

Ответ: НОД$(4321, 1234) = r_5 = 1$.

Такой вариант оформления алгоритма Евклида наиболее пригоден для программирования, а при счете вручную более удобен другой вариант его записи . Вот как он выглядит:



Вычисления оформлены в виде последовательно проводимых делений уголком, остатки обведены в рамочки, а **неполные частные** жирненько выделены. Опять же, НОД - это *последний ненулевой остаток*.

Теперь перейдем ко **второй части задачи**: представить НОД, т.е. 1, как линейную комбинацию чисел $a = 1234$ и $b = 4321$ (найти коэффициенты разложения $1 = 1234x + 4321y$).

Чуть позже мы сможем найти x и y, решив линейное диофантово уравнение с двумя неизвестными, а покуда попросту выразим эти коэффициенты из алгоритма Евклида.

Итак, из равенств $(1) - (6)$ получим выражение НОД (он же r_5) через предыдущие остатки:

$$\text{НОД} = r_5 = \underbrace{r_3 - r_4 \cdot 1}_{\text{из (5)}} =$$

$$\underbrace{(r_1 - r_2 \cdot 1)}_{\text{из (3)}} - \underbrace{(r_2 - r_3 \cdot 153)}_{\text{из (4)}} = \underbrace{r_1 - 2 \cdot r_2 + 153 \cdot r_3}_{\text{упростили}} =$$

$$\underbrace{(b - a \cdot 3)}_{\text{из (1)}} - 2 \cdot \underbrace{(r_2 - r_3 \cdot 153)}_{\text{из (2)}} + 153 \cdot \underbrace{(r_1 - r_2 \cdot 1)}_{\text{из (3)}} =$$

$$\underbrace{b - 5 \cdot a + 155 \cdot r_1 - 153 \cdot r_2}_{\text{упростили}} = b - 5 \cdot$$

$$a + 155 \underbrace{(b - a \cdot 3)}_{\text{из (1)}} - 153 \underbrace{(a - r_1 \cdot 1)}_{\text{из (2)}} =$$

$$\underbrace{156 \cdot b - 623 \cdot a + 153 \cdot r_1}_{\text{упростили}} = 156b - 623a + 153 \underbrace{(b - a \cdot 3)}_{\text{из (1)}} =$$

$$309 \cdot b - 1082 \cdot a$$

Проверка показывает, что действительно

$$1 = 309 \cdot 4321 - 1082 \cdot 1234.$$

Ответ: $x = -1082$ и $y = 309$.

Замечание. Для линейного представления НОДа очень удобен так называемый *расширенный алгоритм Евклида*[1]. Для его реализации сначала необходимо найти все неполные частные $q_0, q_1, ..., q_n$. Значения *u* и *v* вычисляются за несколько шагов, в каждом из которых мы вычисляем r_i в виде $ax_i + by_i$.

Итак, процедура вычисления и таблица для *расширенного алгоритма Евклида* таковы:

[1] EEA – **E**xtended **E**uclidean **A**lgorithm.

$$\left.\begin{aligned} q_{i-1} &= \left[\frac{r_{i-2}}{r_{i-1}}\right] \\ r_i &= r_{i-2} - r_{i-1} \cdot q_{i-1} \\ x_i &= x_{i-2} - x_{i-1} \cdot q_{i-1} \\ y_i &= y_{i-2} - y_{i-1} \cdot q_{i-1} \end{aligned}\right\} \textit{рекуррентные формулы}$$

$$\left.\begin{aligned} r_0 &:= a \\ r_1 &:= b \\ x_0 &:= 1 \\ x_1 &:= 0 \\ y_0 &:= 0 \\ y_1 &:= 1 \end{aligned}\right\} \textit{начальные значения}$$

Мы поменяли местами a и b, поэтому столбцы x_i и y_i тоже надо поменять местами.

i	q_i	r_i	y_i	x_i
0	–	$4321 = b$	1	0
1	3	$1234 = a$	0	1
2	1	619	1	-3
3	1	615	-1	4
4	153	4	2	-7
5	1	3	-307	1075
6	3	**1** = НОД(a, b)	**309** $= y$	**-1082** $= x$

Для проверки результатов, а может быть и для более успешного их получения можно воспользоваться програм-

мой **Mathematica** .

Нам будут полезны следующие функции:

- **GCD[a, b]**. Вычисляет НОД (**G**reatest **C**ommon **D**ivisor) чисел *a* и *b*.

- **Reduce[1234 x+4321y==1,{x,y},Integers]**. Функция **Reduce** умеет решать уравнения и даже неравенства с несколькими переменными. В нашем случае она решает уравнение $x \cdot 1234 + y \cdot 4321 = 1$. В общем случае выглядит так: **Reduce[уравнение,{список переменных},О.Д.З.]**

- **ExtendedGCD[a,b]**. **ExtendedGCD** вычисляет одновременно НОД и коэффициенты его линейного представления в таком виде: {НОД,{*x,y*}}. Это все, что нам нужно найти, но две предыдущие функции не теряют ценности, они еще понадобятся.

Решим нашу задачу.

Вычисление НОД:

input: **a = 1234; b = 4321;**

input: **d = GCD[a, b]**

output: 1

Вычисление коэффициентов линейного представления НОД.

input: **Reduce[x*a+y*b==d,{x,y},Integers]**;

output:

C[1]∈Integers&&x==-1082+4321 C[1]&&y==309-1234 C[1]

Последний результат можно представить в более понятной форме с помощью функции **TraditionalForm**:

input: **TraditionalForm[**$\%$**];**

output: $c_1 \in \mathbb{Z} \wedge x = 4321c_1 - 1082 \wedge y = 309 - 1234c_1$

(Значок $\wedge$ – конъюнкция, означает союз "и".)

Почему в решении присутствует некая буква c_1? Дело в том, что у уравнения $x \cdot 1234 + y \cdot 4321 = 1$ решений бесконечно много, ведь оно зависит от двух переменных, отсюда возникает произвольная константа. Нас устраивает любое решение, поэтому придадим c_1 нулевое значение, чтобы она исчезла и более никого не смущала:

input: **Reduce[x*a+y*b==d,{x,y},Integers]/.C[1]→0**

output: $x = -1082 \wedge y = 309$

И, наконец, более лаконичное решение задачи с помощью функции **ExtendedGCD**:

input: **ExtendedGCD[a,b]**

output: $\{1, \{-1082, 309\}\}$

В *output* ответ представлен в виде двухмерного вектора, первый элемент которого является НОДом, а второй – тоже двухмерным вектором, состоящим из коэффициентов линейного представления НОДа.

1.2 Непрерывные и подходящие дроби

Задача

1. *Найти разложение рационального числа* $\dfrac{3456}{1234}$ *в непрерывную дробь, выписать подходящие дроби.*

2. *Найти разложение иррационального числа* $2 + 3\sqrt{5}$ *в непрерывную дробь.*[1]

Решение первой части задачи.

Для разложения рационального числа $\dfrac{p}{q}$ в непрерывную дробь используется алгоритм Евклида, примененный к числам p и q (именно в таком порядке). На этот раз нам нужны неполные частные $q_0, q_1, ..., q_n$. После их нахождения непрерывная дробь строится следующим образом:

$$\frac{p}{q} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{... + \cfrac{1}{q_n}}}}}$$

Получается, что если известен список неполных частных, то составить непрерывную дробь легко. Поэтому вместо громоздкого представления часто используют более компактное:

$$\frac{p}{q} = [q_0, q_1, ..., q_n].$$

Итак, из алгоритма Евклида находим:

$q_0 = 2$, $q_1 = 1$, $q_2 = 4$, $q_3 = 61$, $q_4 = 2$;

[1] всё необходимое для решения можно найти в книгах Виноградова И.М. (гл. 1) или Дэвенпорта Г.(гл. 4).

$$\frac{3456}{1234} = 2 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{61 + \cfrac{1}{2}}}}$$

или

$$\frac{3456}{1234} = [2, 1, 4, 61, 2].$$

Теперь вычислим подходящие дроби для $\frac{3456}{1234}$. По определению дроби

$$\frac{P_0}{Q_0} = \frac{q_0}{1} \quad ; \qquad \frac{P_1}{Q_1} = q_0 + \frac{1}{q_1} \quad ; \qquad \frac{P_2}{Q_2} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2}} \quad ;$$

$$\frac{P_3}{Q_3} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}}} \quad ; \qquad \frac{P_k}{Q_k} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{... + \cfrac{1}{q_k}}}}}$$

называются подходящими для числа $\frac{p}{q}$. Можно попробовать вычислить их, производя непосредственные преобразования многоэтажных дробей, однако разумнее и проще воспользоваться рекуррентными соотношениями:

$$(1) \quad P_k = P_{k-1} \cdot q_k + P_{k-2};$$
$$(2) \quad Q_k = Q_{k-1} \cdot q_k + Q_{k-2}.$$

Чтобы действовать уж совсем оптимально, составим такую таблицу:

k			0	1	2	3	4
q_k			2	1	4	61	2
P_k	0	1					
Q_k	1	0					

Первые два столбца вспомогательные. Они не нумеруются, всегда выглядят так, как в нашем примере и нужны для корректного запуска вычислений по формулам (1)-(2). Последовательно заполняя пустые места по указанным правилам, найдем

k			0	1	2	3	4
q_k			2	1	4	61	2
P_k	0	1	2	3	14	857	1728
Q_k	1	0	1	1	5	306	617

Итак, числители и знаменатели подходящих дробей вычислены. Для проверки заметим, что последняя подходящая дробь должна совпадать с исходным числом. Так и есть:

$$\frac{3456}{1234} = \frac{1728}{617}.$$

У подходящих дробей много интересных свойств, одно из них таково: эти дроби всегда несократимы. Т.е. последняя дробь представляет исходную дробь в сокращенном виде.

Решение второй части задачи.

Иррациональные числа можно представлять в виде непрерывных дробей почти точно так же, как рациональные. Отличие заключается в том, что дробь в этом случае получается бесконечной:

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{... + \cfrac{1}{q_n + \cfrac{1}{...}}}}}}$$

или $[q_0, q_1, ..., q_n, ...]$. Строго говоря, это предел бесконечной последовательности подходящих дробей. Для превращения любого вещественного числа в непрерывную дробь используется такое представление этого числа:

$$x = [x] + \{x\},$$

где $[x]$ – целая часть x, а $\{x\}$ – дробная. При этом $[x] \geq 1, 0 \leq \{x\} < 1$. Пусть $q_0 = [x]$, а $r_0 = \{x\}$, т.е.

$$x = q_0 + r_0.$$

Запустим алгоритм, аналогичный Евклидову.

$$\frac{1}{r_0} = q_1 + r_1,$$

где

$$q_1 = \left[\frac{1}{r_0}\right], \qquad r_1 = \left\{\frac{1}{r_0}\right\};$$

$$\frac{1}{r_1} = q_2 + r_2, \qquad \left(q_2 = \left[\frac{1}{r_1} \right], \qquad r_2 = \left\{ \frac{1}{r_1} \right\} \right);$$

$$\frac{1}{r_2} = q_3 + r_3, \qquad \left(q_3 = \left[\frac{1}{r_2} \right], \qquad r_3 = \left\{ \frac{1}{r_2} \right\} \right), ...$$

и так далее. Процесс можно описать так: находим дробную часть числа, переворачиваем, находим дробную часть от получившегося, переворачиваем и т.д. Как долго будет длиться это занятие? Трудность заключается в том, что дробь должна получиться бесконечной. Однако для чисел вроде нашего, т.е. квадратичных иррациональностей, дробь будет циклической. На практике разберемся, как разглядеть эту цикличность и как построить непрерывную дробь.

Итак:

$$2 + 3\sqrt{5} = 2 + \sqrt{45} = \underbrace{(2+6)}_{q_0} + \underbrace{(\sqrt{45} - 6)}_{r_0};$$

$$\frac{1}{\sqrt{45} - 6} = \frac{\sqrt{45} + 6}{45 - 36} = \underbrace{1}_{q_1} + \underbrace{\frac{\sqrt{45} - 3}{9}}_{r_1};$$

$$\frac{9}{\sqrt{45} - 3} = \frac{9(\sqrt{45} + 3)}{36} = \frac{\sqrt{45} + 3}{4} = \underbrace{2}_{q_2} + \underbrace{\frac{\sqrt{45} - 5}{4}}_{r_2};$$

$$\frac{4}{\sqrt{45} - 5} = \frac{4(\sqrt{45} + 5)}{20} = \frac{\sqrt{45} + 5}{5} = \underbrace{2}_{q_3} + \underbrace{\frac{\sqrt{45} - 5}{5}}_{r_3};$$

$$\frac{5}{\sqrt{45}-5}=\frac{5(\sqrt{45}+5)}{20}=\frac{\sqrt{45}+5}{4}=\underbrace{2}_{q_4}+\underbrace{\frac{\sqrt{45}-3}{4}}_{r_4};$$

$$\frac{4}{\sqrt{45}-3}=\frac{4(\sqrt{45}+3)}{36}=\frac{\sqrt{45}+3}{9}=\underbrace{1}_{q_5}+\underbrace{\frac{\sqrt{45}-6}{9}}_{r_5};$$

$$\frac{9}{\sqrt{45}-6}=\frac{9(\sqrt{45}+6)}{9}=\sqrt{45}+6=\underbrace{12}_{q_6}+\underbrace{\sqrt{45}-6}_{r_6};$$

Последний остаток r_6 совпал с r_0, а следовательно алгоритм зациклился. Для строительства непрерывной дроби нам нужны $q_0, q_1, ..., q_6$. Следующие значения будут повторяться с периодом длины 6.

$$x=8+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{12+\cfrac{1}{\ddots}}}}}}}$$

или попросту

$$x=[8,(1,2,2,2,1,12)].$$

Скобочки говорят о бесконечной циклической последовательности неполных частных.

Подходящие дроби можно вычислить с помощью алгоритма, приведенного в первой части задачи. Посмотрим, как **Mathematica** справляется с нашей задачей.

Для построения списка неполных частных существует функция **ContinuedFraction[x]**. Вот как она работает:

input: **ContinuedFraction** $[2+3\sqrt{5}]$ *(Ввод функции для нахождения неполных частных.)*

output: $\{8,\{1,2,2,2,1,12\}\}$ *(Ответ в векторном виде.)*

Для функции **ContinuedFractionForm**, которая рисует готовую непрерывную дробь, надо предварительно вызвать специальный пакет:

input: **<< NumberTheory`ContinuedFractions`**

Вот теперь можно рисовать. Аргументом функции **ContinuedFractionForm** служит вектор, состоящий из неполных частных.

input: **ContinuedFractionForm**$[\{8,\{1,2,2,2,1,12\}\}]$

output:

$$8+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{12+\cfrac{1}{\dots}}}}}}}$$

Теперь найдем подходящие дроби.

Функция **ContinuedFractionForm** может иметь второй аргумент, который задает номер этой дроби. Вот первая дробь:

input: **ContinuedFraction** $\left[2+\sqrt{45},1\right]$

output: $\{8\}$

Функция **FromContinuedFraction** считает значение подходящей дроби, если в качестве аргумента подставить вектор из неполных частных.

input: **FromContinuedFraction**[%] *(% на месте аргумента означает последнее вычисленное значение)*

output: 8

Теперь вторая дробь:

input: **ContinuedFraction** $\left[2+\sqrt{45},2\right]$

output: $\{8,1\}$ *(первые два неполные частные)*

input: **FromContinuedFraction[%]**

output: 9 *(вторая подходящая дробь)*

Третья:

input: **ContinuedFraction** $\left[2+\sqrt{45},3\right]$

output: $\{8,1,2\}$

input: **FromContinuedFraction[%]**

output: $\dfrac{26}{3}$ *(третья подходящая дробь)*

И так далее... Если надоело считать подходящие дроби по очереди, можно получить их все разом, использовав функцию **Table**.

input:

Table[FromContinuedFraction[ContinuedFraction[$2+\sqrt{45}$**,n]], {n,1,6}]**

output: $\left\{8,9,\dfrac{26}{3},\dfrac{61}{7},\dfrac{148}{17},\dfrac{209}{24}\right\}$ *(список всех подходящих дробей.)*

1.3 Линейное диофантово уравнение

Задача. *Решить диофантово уравнение*

$$150x+168y=24,$$

используя подходящие дроби.

Решение. При решении диофантова уравнения мы будем опираться на два ключевых факта.

1. *Диофантово уравнение $ax + by = c$ разрешимо тогда и только тогда, когда его правая часть c делится на $d =$НОД(a, b).*

2. *Если x_0 и y_0 – какая-либо пара целых решений уравнения $ax + by = c$, то общее решение этого уравнения выглядит так:*

$$x = x_0 + C \cdot \frac{b}{d} \quad , \qquad y = y_0 - C \cdot \frac{a}{d}$$

где C – произвольная целая константа.

В нашем случае $d = 6$, очевидно, $24 \ \vdots \ 6$ и уравнение разрешимо. Сократим уравнение на 6, получим

$$25x + 28y = 4.$$

Решим вспомогательное уравнение

$$25x' + 28y' = 1.$$

По сути оно является линейным представлением НОД$(25, 28)$, т.е. единицы. Здесь нам потребуется третье утверждение:

3. *Для того, чтобы выразить d =НОД(a, b) в виде линейной комбинации чисел a и b формулой*

$$ax^{/} + by^{/} = d,$$

надо, разложив дробь $\frac{a}{b}$ в непрерывную, составить подходящую дробь $\frac{P_{n-1}}{Q_{n-1}}$. Тогда

$$x^{/} = (-1)^{n-1}Q_{n-1} \quad , \qquad y^{/} = (-1)^{n}P_{n-1},$$

где C – произвольная целая константа.

При разложении $\frac{25}{28}$ в непрерывную дробь, получим:

$$\frac{25}{28} = [0, 1, 8, 3].$$

Нумерация подходящих дробей начинается с нуля, поэтому предпоследней является дробь номер два.

$$\frac{P_2}{Q_2} = \frac{8}{9} \quad ,$$

$$x^{/} = (-1)^2 \cdot Q_2 \quad , \qquad y^{/} = (-1)^3 \cdot P_2,$$
$$x^{/} = 9 \quad , \qquad y^{/} = -8.$$

Вернемся к уравнению $25x + 28y = 4$. Его неизвестные связаны с $x^{/}$ и $y^{/}$ равенствами:

$$x = 4 \cdot x^{/}, \quad y = 4 \cdot y^{/}.$$

Ответ: $x = 9 \cdot 4 + 28 \cdot C \quad , \qquad y^{/} = -8 \cdot 4 - 25 \cdot C.$

Решение диофантова уравнения с помощью функции **Reduce[уравнение,{список переменных},О.Д.З.]** в **Mathematica** уже рассматривалось при разборе **задачи 1**.

1.4 Разложение на простые множители

Определение. Натуральное число $n > 1$ называется простым числом, если у него нет делителей, отличных от 1 и от самого числа n.

Определение. Натуральное число $n > 1$ называется составным числом, если оно имеет делитель, отличный от 1 и n.

Свойство 1. Пусть p – наименьший делитель среди неединичных делителей числа $n > 1$. Тогда p – простое число.

Свойство 2. Пусть p – наименьший делитель среди неединичных делителей составного числа n. Тогда $p < \sqrt{n}$.

Теорема 4 (Основная теорема арифметики)**.** *Произвольное натуральное число $n > 1$ можно представить в виде произведения простых чисел. Это представление однозначно с точностью до порядка сомножителей*[1].

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k} = \prod_{i=1}^{k} p_i^{e_i}.$$

[1]Вот почему число 1 не считается простым! В противном случае его можно было бы включить в это разложение с любой степенью.

Теорема 5. *Всякое составное число* n *имеет делитель* $q \leq n$.

Задача 1. *Разложить число* n *на простые множители.*[2]

Первый способ разложения на простые множители – **перебор**, основанный на **свойствах 1** и **2**. Он заключается в следующем: число *n* последовательно делится на простые числа, не превосходящие $\sqrt{n}$. При этом , если *n* делится на простое *p* без остатка, число *p* помещается в список простых делителей, *n* делится на *p* и к частному вновь применяется тот же алгоритм. Этот способ годится для разложения не слишком больших чисел, для которых реально проверить список возможных делителей с помощью таблицы простых чисел.

Пример: $n = 25800840$.

Решение. Испытаем делимость этого числа на простые числа 2, 3, 5, 7, 11, 13 и т.д. Результаты удобно расположить в виде таблицы.

[2]Перед решением этой задачи полезно ознакомиться с теоретическими основами, например по книгам Виноградова И.М. (гл. 1) или Дэвенпорта Г.(гл. 1).

2	12900420
2	6450210
2	3225105
3	1075035
3	358345
5	71669
13	5513
37	149
149	1

В левом столбце таблицы записаны простые делители, а в правом результаты последовательного деления числа 25800840 на эти делители. Итак, искомое разложение:

$$25800840 = 2^3 \cdot 3^2 \cdot 5 \cdot 13 \cdot 37 \cdot 149$$

Однако, если наименьший простой делитель числа n достаточно велик (близок к $\sqrt{n}$), то **алгоритм перебора** может оказаться трудоёмким или вообще не привести к успеху. В таком случае более эффективным может оказаться **алгоритм Ферма**. Основная идея этого алгоритма заключается в том, чтобы представить *n* в виде

$$n = x^2 - y^2 = (x - y)(x + y)$$

где *x* и y – неотрицательные целые числа. Тогда $x + y$ и $x - y$ являются делителями числа *n*. Пошагово алгоритм Ферма выглядит так:

Шаг 1. Берем натуральное нечетное число *n*. (Если *n* четное, то, очевидно, 2 его делитель).

Шаг 2. Присваиваем *x* значение целой части $\sqrt{n}$:

$$x := [\sqrt{n}]$$

Если $n = x^2$, то x является делителем числа n и алгоритм привел к успеху. В противном случае увеличиваем x на 1 и переходим к шагу 3.

Шаг 3. Если $x = (n+1)/2$, то число n простое и работа алгоритма останавливается. В противном случае вычисляем $y = \sqrt{x^2 - n}$.

Шаг 4. Если y целое число, то мы получили требуемое разложение $n = x^2 - y^2 = (x-y)(x+y)$ и работа алгоритма закончена. В противном случае увеличиваем x на 1 и переходим к шагу 3.

Пример. $n = 1\,342\,127$.

Решение. Сначала переменной x присваиваем значение целой части $\sqrt{1\,342\,127}$, т.е. $x = 1158$. Тогда $x^2 = 1\,340\,964 \neq 1\,342\,127$. Поэтому увеличиваем значение x на 1 и переходим к шагу 3. Вычисляем значение $(n+1)/2 = 671\,064$, сравниваем с x (очевидно, они не равны) и проверяем, является ли целым $y = \sqrt{x^2 - n}$. Значения x и y в конце каждого цикла записываем в таблицу:

x	$y = \sqrt{x^2 - n}$
1159	33.97...
1160	58.93...
1161	76.11...
1162	90.09...
1163	102.18...
1164	113

Итак, на шестом цикле получили целые значения x и y: $x = 1164$, $y = 113$. Следовательно множители равны

$$x + y = 1277 \text{ и } x - y = 1051.$$

Алгоритм Ферма дает хорошие результаты, когда значения делителей числа *n* различаются не слишком сильно, иначе количество проводимых циклов становится настолько велико, что все преимущества этого метода исчезают. Ну а более общие случаи разложения на простые множители требуют и более изощренных алгоритмов, изложение которых не предполагается в данном курсе. Однако плодами высокой науки может воспользоваться даже неискушенный исследователь, если у него имеется возможность проводить свои вычисления с помощью современных компьютерных программ, например с помощью пакета **Wolfram Mathematica** или сайта **WolframAlpha**.

Приведем решение задачи разложения на простые множители в этом пакете.

Пример. $n = 708207257160$

Решение. В **Mathematica** для разложения числа *n* на простые множители существует функция **FactorInteger[n]**, результатом применения которой будет список простых делителей ***n*** с учетом их кратности (степени) в разложении.

Ввод (input): $n = 708207257160$

Результат (output): 708207257160

Ввод (input): **FactorInteger[n]**

Результат (output):

$$\{\{2, 3\}, \{3, 2\}, \{5, 1\}, \{13, 1\}, \{37, 1\}, \{149, 1\}, \{27449, 1\}\}$$

Итак,

$$708207257160 = 2^3 \cdot 3^2 \cdot 5 \cdot 13 \cdot 37 \cdot 149 \cdot 27499.$$

Заметим, что число 27499 является простым, что весьма затруднительно проверить вручную, но с легкостью проверяется **Mathematica** с помощью функции **PrimeQ[n]**, которая непринужденно выясняет простоту числа *n*:

Ввод (input) : **PrimeQ[27449]**

Результат (output): True

Ввод (input) : **PrimeQ[1024]**

Результат (output): False

1.5 Функция Эйлера

Задача.*Вычислить значение функции Эйлера для чисел:* a_1, a_2, a_3.

Решение. Функция Эйлера для натурального числа *n* это количество чисел из ряда

$$0, 1, 2, 3, ..., n-1,$$

взаимно простых с *n*. Формула, позволяющая вычислять значение функции Эйлера $\varphi(n)$, зависит от списка простых делителей числа *n* $p_1\,, p_2\,, ...,\, p_k$:

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_k}\right).$$

Если число p простое, то для него формула упрощается:

$$\varphi(p) = p - 1.$$

Другой частный случай:

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1},$$

где p опять же простое.

Кроме того функция Эйлера мультипликативна, т.е.

$$\varphi(n_1 \cdot n_2) = \varphi(n_1) \cdot \varphi(n_2).$$

Вобщем, все просто, если мы знаем каноническое разложение n. Но в том-то и заключается проблема, что найти простые делители большого числа очень и очень сложно. На этой сложности основаны многие алгоритмы криптографии (шифрования). При решении этой задачи вполне оправдано применение компьютера.

Можно воспользоваться готовой функцией Эйлера **EulerPhi[a]**:

input: **EulerPhi[234]** *(Функция Эйлера для 234.)*

output: **72**

Посмотрим на список чисел, взаимно простых с числом 234, они же образуют приведенную систему вычетов по модулю 234. Для этого воспользуемся функцией **Select**, которая из списка чисел от 1 до 234 (задается с помощью **Range [234]**) выбирает числа, взаимно простые с 234 (**GCD [#1 , 234] == 1&** – критерий выбора).

input: **Select [Range [234], GCD [#1 , 234] == 1&]**

output: **{1,5,7,11,17,19,23,25,29,31,35,37,41,43,**
47,49,53,55,59,61,67, 71,73,77,79,83,85,89,95,97,101,
103,107,109,113,115,119,121,125,
127,131,133,137,139,145,149,151,155,
157,161,163,167,173,175,179,
181,185,187,191,193,197,199,203,205,
209,211,215,217,223,227,229,233}

Количество этих чисел 72, т.е. $\varphi(234) = 72$.

1.6 Системы вычетов

Задача. *Найти наименьшие положительные и наименьшие абсолютные вычеты по модулю 11 чисел:* $3, 8, 17, -17, 120, 54, -40, 236, 237$. *Какие из этих чисел сравнимы по модулю 11?*

Решение. Наименьший положительный вычет числа a по модулю m – это остаток при делении a на m. Поэтому ответом на первый вопрос будет список остатков[1] предъявленных чисел:

$$3, 8, 6, 5, 10, 10, 4, 5, 6.$$

Очевидно, что наименьший абсолютный вычет – это минимальный по абсолютной величине представитель класса вычетов по данному модулю. Устные вычисления

[1]Напоминание: остаток неотрицателен и строго меньше делителя.

показывают, что ответ на второй вопрос будет таким:

$$3, -3, -5, 5, -1, -1, 4, 5, -5.$$

(Сравниваем два вычета: наименьший положительный r и $r - m$, выбираем наименьший по абсолютной величине.)

Поскольку оба упомянутых вида вычетов задаются однозначно, с их помощью легко найти сравнимые числа. Это 17 и 237, -17 и 236, 120 и 54.

Для работы в **Mathematica** подойдет функция **Mod[a, m]**, которая применима не только к числам , но и векторам **a**.

input: **Mod[{3,8,17,-17,120,54,-40,236,237},11]**

output: **{3,8,6,5,10,10,4,5,6}** *(наименьшие положительные вычеты.)*

1.7 Вычисление степеней в $\mathbb{Z}_m$

Задача. *Найти остаток от деления степенного выражения 3^{567} на число 7.*

Решение. Найдем остатки от деления степеней числа

3 на 7.

3^k	остаток при делении на 7
3^0	$1(mod\,7) = \mathbf{1}$
3^1	$\mathbf{1} \cdot 3(mod\,7) = \mathbf{3}$
3^2	$\mathbf{3} \cdot 3(mod\,7) = \mathbf{2}$
3^3	$\mathbf{2} \cdot 3(mod\,7) = \mathbf{6}$
3^4	$\mathbf{6} \cdot 3(mod\,7) = \mathbf{4}$
3^5	$\mathbf{4} \cdot 3(mod\,7) = \mathbf{5}$
3^6	$\mathbf{5} \cdot 3(mod\,7) = \mathbf{1}$

Далее остатки будут циклически повторяться с периодом 6:

$$3^{k+6}(mod\,7) = 3^k(mod\,7)$$

Степень 567 при делении на 6 дает остаток 3:

$$567(mod\,6) = 3,$$

поэтому

$$3^{567}(mod\,7) = 3^3(mod\,7) = 6.$$

В **Mathematica** для нахождения остатка от деления числа *a* на *m* существует функция **Mod[a, m]**. Для вычисления остатка от деления степенного выражения a^b на число *m* можно использовать **PowerMod[a, b, m]**.

1.8 Обратный элемент в $\mathbb{Z}_m$

Задача. *Найти вычет, обратный к вычету* **a** *по модулю* **m***:*

1) *с помощью расширенного алгоритма Евклида (a=13, m=32);*

2) *с помощью теоремы Эйлера (a=61, m=426).*

Решение. Вычеты по данному модулю образуют множество, замкнутое относительно действий сложения и умножения (такие множества в математике называют *кольцами*). Это означает, что результат сложения или умножения двух вычетов также является вычетом по тому же модулю. Если вдруг оказалось, что произведение вычетов *a* и *b* равно 1, т.е.

$$\overline{a} \cdot \overline{b} = \overline{1},$$

или, что то же самое

$$a \cdot b \equiv 1 (mod\, m),$$

то *a* и *b* называют взаимно обратными вычетами и обозначают это обстоятельство так:

$$\overline{a} = (\overline{b})^{-1}, \; \overline{b} = (\overline{a})^{-1}.$$

Все это означает, что в кольце вычетов можно ввести действие деления, т.е. умножение на обратный элемент.

$$\frac{\overline{a}}{\overline{b}} = \overline{a} \cdot (\overline{b})^{-1}.$$

Однако обратимыми оказываются отнюдь не все элементы кольца вычетов, а только взаимно простые с модулем.

Решение 1-й части задачи.

$a^{-1}(mod\, m)$ является решением сравнения

$$ax \equiv 1(mod\, m).$$

В свою очередь это сравнение эквивалентно линейному диофантову уравнению $ax + my = 1$. Решим его, использовав расширенный алгоритм Евклида:

i	q_i	r_i	x_i
0	–	$32 = m$	0
1	2	$13 = a$	1
2	2	6	-2
3	6	1	5

Здесь мы учли, что вторую неизвестную y находить не надо.

Итак, $a^{-1}(mod\, m) = x_3 = 5$.

Для **решения второго пункта** задачи нам понадобится ***теорема Эйлера:***

Для любого числа a, взаимно простого с модулем m (простым или составным), имеет место сравнение

$$a^{\varphi(m)} \equiv 1\,(mod\, m)$$

Понятно, что в качестве обратного к *a* надо взять $a^{\varphi(m)-1}$.

Таким образом, план решения следующий:

1. Убеждаемся, что *a* взаимно просто с *m*.

2. Находим $\varphi(m)$.

$\varphi(426) = 140$.

3. Вычисляем $a^{\varphi(m)-1}(mod\, m)$.

$61^{139}(mod\, 426) = 7$. Как получен этот результат? Вручную вычисления можно построить следующим образом:

$61^2(mod\, 426) = 313$

$61^4(mod\, 426) = 313^2(mod\, 426) = 415(mod\, 426) = -11(mod\, 426)$

$61^8(mod\, 426) = (-11)^2(mod\, 426) = 121(mod\, 426)$

$61^{16}(mod\, 426) = 121^2(mod\, 426) = 157(mod\, 426)$

$61^{32}(mod\, 426) = 157^2(mod\, 426) = 367(mod\, 426) = -59(mod\, 426)$

$61^{64}(mod\, 426) = (-59)^2(mod\, 426) = 73(mod\, 426)$

$61^{128}(mod\, 426) = 73^2(mod\, 426) = 217(mod\, 426)$

$139 = 128 + 8 + 1 \Rightarrow 61^{139}(mod\, 426) = 61^{128+8+1}(mod\, 426) = 61^{139} \cdot 61^8 \cdot 61^1(mod\, 426) = 7$

4. Проверка: $61 \cdot 7(mod\, 426) = 1$

1.9 Сравнения первой степени

Задача. *Решить сравнение первой степени*

$$32x \equiv 14\,(mod\, 69).$$

Решение. Сравнение вида $ax \equiv b\,(mod\, m)$ разрешимо, если b делится на НОД$(a, m) = d$. При этом оно имеет ровно d решений.

Кроме того, если коэффициент a и модуль m взаимно просты, то решение сравнения можно получить в таком виде:

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

где a^{-1} вычет, обратный к a по модулю m.

Как было показано в предыдущей задаче,

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

В нашем случае получаем:

$$32^{-1} (mod\, 69) \equiv 32^{44-1} (mod\, 69) \equiv 41 (mod\, 69).$$

Отсюда вычисляем ответ:

$$x \equiv 41 \cdot 14 (mod 69) \equiv 22 (mod\, 69).$$

Вроде бы ответ получен просто и быстро, однако, на самом деле вручную проводить такие вычисления довольно утомительно (например $32^{43} (mod\, 69)$). Другой способ решения сравнения первой степени заключается в применении непрерывных дробей. А именно:

$$x = (-1)^n \cdot P_{n-1} \cdot b\, (mod\, m),$$

где P_{n-1} числитель предпоследней подходящей дроби для $\dfrac{m}{a}$.

$$\frac{69}{32} = [2, 6, 2, 2] = 2 + \cfrac{1}{6 + \cfrac{1}{2 + \cfrac{1}{2}}}$$

Заполним таблицу для нахождения P_k:

k			0	1	2	3
q_k			2	6	2	2
P_k	0	1	2	13	28	

Предпоследним является номер два ($n-1=2$), поэтому

$$x = (-1)^3 \cdot 28 \cdot 14 (mod\, 69) = -392 (mod\, 69) = 22.$$

Все вычисления проводятся вручную и вобщем-то устно.

Проверка: $32 \cdot 22\,(mod\, 69) \equiv 14\,(mod\, 69)$.

1.10 Система линейных сравнений

Задача. *Решить систему сравнений первой степени с помощью китайской теоремы об остатках.*

$$\begin{cases} x \equiv 41 (mod\, 59) \\ x \equiv 1 (mod\, 9) \\ x \equiv 2 (mod\, 121) \end{cases}$$

Решение. ***Китайская теорема об остатках:*** *Пусть $m_1, m_2, ..., m_k$ – попарно взаимно простые числа > 1, $M = m_1 m_2 ... m_k$. Тогда существует единственное решение в кольце вычетов по модулю M системы сравнений:*

$$\begin{cases} x \equiv a_1 (mod\, m_1) \\ x \equiv a_2 (mod\, m_2) \\ \quad ..... \\ x \equiv a_k (mod\, m_k) \end{cases}$$

При этом решение можно представить в виде:

$$x = q_1 + q_2 \cdot m_1 + q_3 \cdot m_1 \cdot m_2 + ... + q_k \cdot m_1 \cdot m_2 ... m_{k-1}, \ (\star)$$

где $0 \leq q_i < |m_i|$, $q_1 = a_1 (mod\, m_1)$.

Таким образом, наша задача – найти коэффициенты q_1, q_2, q_3 из формулы $(\star)$.

1) $q_1 \equiv a_1 (mod\, m_1) \equiv 41 (mod\, 59) \equiv 41.$

2) $q_2 \cdot m_1 \equiv x - q_1 (mod\, m_2) \Longrightarrow$
$59 \cdot q_2 \equiv x - 41 (mod\, 9) \Longrightarrow$
$59 \cdot q_2 \equiv x (mod\, 9) - 41 (mod\, 9) \Longrightarrow$
$59 \cdot q_2 \equiv 1 - 5 (mod\, 9) \Longrightarrow$
$59 \cdot q_2 \equiv 5 (mod\, 9)$
Это сравнение первой степени, которое имеет решение
$q_2 = 5 \cdot 59^{-1} (mod\, 9) = 1$

3) $x - q_1 - q_2 \cdot m_1 \equiv q_3 \cdot m_1 \cdot m_2 (mod\, m_3) \Longrightarrow$
$q_3 \cdot 9 \cdot 59 \equiv x - 41 - 1 \cdot 59 (mod\, 121) \Longrightarrow$
$47 \cdot q_3 \equiv -98 (mod\, 121) \Longrightarrow$
$q_3 \equiv 70 (mod\, 121)$

Итак,

$$x = 41 + 1 \cdot 59 + 70 \cdot 59 \cdot 9 = 37270.$$

Проверка показывает, что ответ верный:

$$\begin{cases} 37270 \equiv 41 (mod\, 59) \\ 37270 \equiv 1 (mod\, 9) \\ 37270 \equiv 2 (mod\, 121) \end{cases}$$

Другой способ решения системы линейных сравнений использует такую формулу для вычисления x :

$$x = x_1\alpha_1 M_1 + x_2\alpha_2 M_2 + \ldots + x_k\alpha_k M_k (mod\, M),$$

где $M_i = \dfrac{M}{m_i}$, $\alpha_i = M_i^{-1}(mod\, M_i)$, $x_i = x(mod\, m_i)$.

Вычислим $M_1,\ M_2,\ M_3$:

$$M_1 = m_2 m_3 = 9 \cdot 121 = 1089;$$
$$M_2 = m_1 m_3 = 59 \cdot 121 = 7139;$$
$$M_3 = m_1 m_2 = 59 \cdot 9 = 531.$$

Теперь вычислим обратные значения:

$$\alpha_1 = M_1^{-1}(mod\, 59) = 1089^{-1}(mod\, 59) = 27^{-1}(mod\, 59) = 35;$$
$$\alpha_2 = M_2^{-1}(mod\, 9) = 7139^{-1}(mod\, 9) = 2^{-1}(mod\, 9) = 5;$$
$$\alpha_3 = M_3^{-1}(mod\, 121) = 531^{-1}(mod\, 121) = 47^{-1}(mod\, 121) = 103.$$

Найдем x :

$$x = x_1\alpha_1 M_1 + x_2\alpha_2 M_2 + x_3\alpha_3 M_3 =$$
$$= 41 \cdot 35 \cdot 1089 + 1 \cdot 5 \cdot 7139 + 2 \cdot 103 \cdot 531 (mod\, M) =$$
$$= 1707796 (mod\, 64251) = 37270.$$

Mathematica тоже умеет решать системы сравнений первой степени. Для использования функции **ChineseRemainder[list1,list2]** сначала необходимо вызвать пакет **NumberTheoryFunctions**:

input: **<< NumberTheory`NumberTheoryFunctions`**

input: **ChineseRemainder[{41 ,1 ,2 }, {59 ,9 ,121 }]**

output: $\{37270\}$

1.11 Алгоритм шифрования RSA

Задача. *Зашифровать и расшифровать сообщение с помощью криптосистемы RSA (R. Rivest, A. Shamir, L. Adleman). Даны простые числа* $p = 353$ *и* $q = 467$ *(закрытая часть ключа) и сообщение* $M = 25$. *Требуется выбрать вторую часть открытого ключа e,построить третью часть закрытого ключа d, зашифровать и расшифровать сообщение*

Решение. В схеме RSA в качестве множества исходных и зашифрованных сообщений используется кольцо вычетов по модулю $n = p \cdot q$, где *p* и *q* – большие простые числа (в реальности число знаков в их десятичной записи превосходит 100.) Алгоритм работы данной криптосистемы следующий:

1. Получатель (владелец секретной части ключа *p* и *q*) вычисляет значение функции Эйлера $\varphi(n)$. В нашей задаче

$$n = 353 \cdot 467 = 164851,$$

$$\varphi(164851) = (353 - 1)(467 - 1) = 164032$$

Число *n* является первой частью открытого ключа. Поскольку оно очень большое, вычислить его функцию Эйлера, не зная разложения на простые множители, практически невозможно.

2. Получатель генерирует случайный элемент *e* в кольце вычетов по модулю $\varphi(n)$, такой, что он обратим в этом кольце (т.е. взаимно прост с $\varphi(n)$). Пара чисел *(n, e)* является открытым ключом и рассылается всем адресатам по открытым каналам.

Итак, мы в качестве e можем взять любое, лучше маленькое число, взаимно простое с $\varphi(164851) = 164032$. Пусть $e = 3$, т.к. 164032 очевидно не делится на 3.

3. Шифрование сообщения M состоит в возведении его в степень e в кольце вычетов по модулю n.

$$C = M^e \,(mod\, n\,) = 25^3 \,(mod\, 164851\,) = 15625.$$

Зашифровать сообщение может всякий, кто получил открытый ключ.

4. Для e вычисляется обратный элемент d в кольце вычетов по модулю $\varphi(n)$.

$$d \cdot e \equiv 1 \,(mod\, \varphi(n)\,).$$

Пара *(n, d)* – секретный ключ. Естественно, найти d может только тот, кто знает функцию Эйлера числа n(конечно, если он умеет решать сравнения первой степени). Ну, чтож, попробуем:

$$d \cdot 3 \equiv 1 \,(mod\, \varphi(164032)\,) \Rightarrow d = 109355.$$

5. Чтобы расшифровать C, возведем его в степень d в кольце вычетов по модулю n.

$$S = C^d \,(mod\, n\,) = 15625^{109355} \,(mod\, 164851\,) = 25.$$

Замечание. Вычисления, выполненные в пункте **5** производят тяжелое впечатление, особенно, если учесть,

что в реальной задаче шифрования используют стозначные модули *n*. Даже компьютер призадумается над таким вычислением. На помощь приходит древняя, но по-прежнему актуальная *китайская теорема об остатках*. Поскольку нам известно секретное разложение модуля *n* на множители *p* и *q*, мы можем сопоставить числу *C* его остатки при делении на эти числа[1] или CRT-разложение[2]

$$C \longleftrightarrow (C(mod\, p), C(mod\, q)),$$

т.е. в нашем случае

$$15625 \longleftrightarrow (15625(mod\, 353), 15625(mod\, 467)) =$$

$$= (93(mod\, 353), 214(mod\, 467)).$$

Теперь возведем в степень $d = 109355$ каждый элемент этой пары. Поскольку модули *p* и *q* простые, можем сократить степени до остатков по модулям *p-1* и *q-1* соответственно.

$$93^{109355(mod\, 352)}(mod\, 353) \equiv 93^{235}(mod\, 353) = 25(mod\, 353)$$

(Последнее вычисление можно провести способом, указанном в **задаче 8.**)

$$214^{109355(mod\, 466)}(mod\, 467) \equiv 214^{311}(mod\, 467) = 25(mod\, 467)$$

Мы получили, что

$$C^d \longleftrightarrow (25(mod\, 353), 25(mod\, 467)).$$

[1] Причем это сопоставление взаимнооднозначно в кольце вычетов по модулю *n*.

[2] **C**hinese **R**emainder **T**heorem

Восстановим значение C^d, решив систему из двух сравнений:

$$C^d = q_1 + q_2 \cdot 352,$$

$$q_1 = 25,$$

$$q_2 \cdot 352 \equiv 25 - 25 (mod\, 466) \Longrightarrow$$

$$q_2 \equiv 0 (mod\, 466) \Longrightarrow$$

$$C^d = 25.$$

Мы применили схему вычислений в кольце вычетов по большому модулю $n = p \cdot q$, построенную на применении *китайской теоремы об остатках*:

$$\begin{array}{ccc} C & \xrightarrow{\text{CRT-разложение}} & (C(mod\, p), C(mod\, q)) \\ & & \downarrow \\ C^d & \xleftarrow[\text{китайская теорема об остатках}]{} & (C^d(mod\, p), C^d(mod\, q)) \end{array}$$

Несмотря на то, что эта схема выглядит, как обходной маневр, ее реализация приводит к сокращению объемов вычислений в 3-4 раза.

1.12 Индексы, первообразные корни

Задача.

1) *Для простого модуля $m = 31$ найти первообразный корень и составить таблицу индексов для приведенной системы вычетов по модулю 31.*

2) *С помощью таблицы индексов решить сравнение*

$$15 \cdot 21^x \equiv 19\,(mod\,31).$$

Решение. 1) Для начала разберемся с основными понятиями, коими являются первообразный корень и индексы.

Итак, нам дано простое число *31*. Приведенной системой вычетов для него будет

$$\overline{1},\ \overline{2},\ \overline{3},\ ...,\ \overline{30}\,,$$

т.к. эти вычеты взаимно просты с *31*. Из теоремы Ферма следует, что любой вычет $\overline{a}$ из приведенной системы при возведении в степень *30* сравним с единицей по модулю *31*.

$$a^{\varphi(31)} \equiv a^{30} \equiv 1(mod\,31).$$

Однако это не значит, что *30* – это наименьшая степень, обладающая таким свойством. Проведем эксперимент: возьмем вычет $\overline{2}$ и начнем возводить его в разные степени в кольце вычетов по модулю *31*.

$$2^1 \equiv 2(mod\,31)$$

$$2^2 \equiv 4(mod\,31)$$

$$2^3 \equiv 8(mod\,31)$$

$$2^4 \equiv 16(mod\,31)$$

$$2^5 \equiv 1(mod\,31)$$

Вот так, не добравшись до степени $\varphi(31) = 30$, мы уже получили единицу.

Определение 1. *Наименьшая степень k, для которой выполняется*

$$a^k \equiv 1 \,(mod\, m)$$

называется показателем числа a по модулю m.

(показатель $\overline{2}$ равен 5)

Определение 2. *Число a, взаимно простое с модулем m, называется первообразным корнем по модулю m, если его показатель по модулю m равен $\varphi(m)$.*

($\overline{2}$ не является первообразным корнем по модулю 31.)

Все это означает, что для каждого вычета $\overline{a}$ из приведенной системы есть две возможности:

1. При возведении его в степени мы получим единицу, только добравшись до степени $\varphi(m)$, и тогда это первообразный корень. При этом

$$\overline{a^1},\ \overline{a^2},\ \overline{a^3},\ ...,\ \overline{a^{\varphi(m)}}$$

тоже образуют приведенную систему вычетов, расставленных в некоем новом порядке.

2. Как и в нашем эксперименте над вычетом *2* по модулю *31* получаем, что показатель меньше $\varphi(m)$.

Замечание. *На самом деле в этом случае показатель принимает отнюдь не какие угодно значения, он обязан быть делителем $\varphi(m)$, т.е. в нашем случае числа 30. Так и есть:* $30 \vdots 5$.

Теперь отправляемся на поиски первообразного корня для модуля *31*. Следующий кандидат – вычет *3*. Испытаем его:

$$3^1 \equiv 3(mod\,31)$$
$$3^2 \equiv 9(mod\,31)$$
$$3^3 \equiv 27(mod\,31)$$
$$3^4 \equiv 19(mod\,31)$$
$$3^5 \equiv 26(mod\,31)...$$

Неужели придется вычислять все *30* степеней? Если мы примем во внимание выделенное курсивом замечание, то сможем ограничиться проверкой только степеней, являющихся делителями числа *30*.

$$3^6 \equiv 16(mod\,31)$$
$$3^{10} \equiv 3^{5+5} \equiv 25(mod\,31)$$
$$3^{15} \equiv 3^{10+5} \equiv 21(mod\,31)$$

Итак, показателем оказалась степень *30*, следовательно *3* – первообразный корень.

Еще одно замечание: *Не у любого модуля имеется первообразный корень (к примеру у 8 такового нет). Впрочем, если модуль простой, то все в порядке*[1]. *У него может оказаться даже несколько первообразных корней.*

Пусть p – простое число, a не делится на p, и γ – первообразный корень по модулю p.

Определение 3. *Число* $k \geq 0$ *называется индексом числа a по основанию* γ, если

$$\gamma^k \equiv a\,(mod\,m).$$

[1]Еще более точно так: у числа n есть первообразные корни тогда и только тогда, когда оно имеет вид $2, 4, p^\alpha$ или $2p^\alpha$, где p – нечетное простое число.

Обозначение: $k = ind_\gamma a$ или просто $ind\, a$, т.к. обычно в качестве первообразного корня берут наименьший из имеющихся.

В иностранной литературе индексы чаще называют *дискретными логарифмами*, и это не удивительно, ведь свойства индексов и логарифмов почти идентичны.

Составим таблицу индексов по основанию *3* для модуля *31*. Для этого надо честно возвести *3* во все степени от *2* до *30*. Прилежным вычислениям в очередной раз поможет **Mathematica** .

input: **PrimitiveRoot[31]**
(еще раз находим наименьший первообразный корень для 31)

output: 3 *(мы так и знали!)*

input: **deg = Table[{*i*, Mod[3^*i*, 31]}, {*i*, 2, 31}]**
(*находим степени для всех вычетов из приведенной системы и составляем таблицу, состоящую из таких пар:* $\{i,\ 3^i\ (mod\, 31)\}$)

output: $\{\{2,9\},\{3,27\},\{4,19\},\{5,26\},\{6,16\},\{7,17\},$
$\{8,20\},\{9,29\},\{10,25\},\{11,13\},\{12,8\},\{13,24\},$
$\{14,10\},\{15,30\},\{16,28\},\{17,22\},\{18,4\},\{19,12\},$
$\{20,5\},\{21,15\},\{22,14\},\{23,11\},\{24,2\},\{25,6\},$
$\{26,18\},\{27,23\},\{28,7\},\{29,21\},\{30,1\},\{31,3\}\}$
(Получилась такая таблица. Ее можно сделать более внятной, если применить к ней функцию **TableForm[deg]***, однако из соображений экономии места здесь мы этого делать не будем.)*

input: **index = Map[Reverse, ind]**
(Функция **Reverse** *меняет порядок элементов в одномерном списке; функция* **Map[func, list]** *воздействует функцией* **func** *на каждый элемент списка* **list***.)*

output: $\{\{9,2\},\{27,3\},\{19,4\},\{26,5\},\{16,6\},\{17,7\},$
$\{20,8\},\{29,9\},\{25,10\},\{13,11\},\{8,12\},\{24,13\},$
$\{10,14\},\{30,15\},\{28,16\},\{22,17\},\{4,18\},\{12,19\},$
$\{5,20\},\{15,21\},\{14,22\},\{11,23\},\{2,24\},\{6,25\},$
$\{18,26\},\{23,27\},\{7,28\},\{21,29\},\{1,30\},\{3,31\}\}$
(Эта таблица обратна первой: в ней каждому вычету сопоставлен его индекс $\{i,\ ind_3\, i\}$. Однако вычеты идут не по порядку. Исправим этот недостаток.)

input: **Sort[index]**
(Функция **Sort[list]** *сортирует элементы списка* **list** *в порядке возрастания.)*

output: $\{\{1,30\},\{2,24\},\{3,31\},\{4,18\},\{5,20\},\{6,25\},$
$\{7,28\},\{8,12\},\{9,2\},\{10,14\},\{11,23\},\{12,19\},$
$\{13,11\},\{14,22\},\{15,21\},\{16,6\},\{17,7\},\{18,26\},$
$\{19,4\},\{20,8\},\{21,29\},\{22,17\},\{23,27\},\{24,13\},$
$\{25,10\},\{26,5\},\{27,3\},\{28,16\},\{29,9\},\{30,15\}\}$
(Готовая таблица индексов.)

Замечание: Таблицы индексов и обратные к ним получаются длинными и тонкими, что неудобно. В связи с этим издревле их принято оформлять так:

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									

Это **таблица индексов**. Номер строки означает число десятков, а номер столбца – число единиц N. Чтобы получить к примеру индекс числа 14, находим пересечение 1-ой строчки и 4-го столбца. Ответ – 22.

Обратная таблица, с помощью которой, зная индекс, можно найти исходное число:

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

Пользуемся ей так. Предположим, индекс некого числа равен 11. На пересечении строчки № 1 и столбца № 1 находится число 13.

2)Решим сравнение $15 \cdot 21^x \equiv 19\,(mod\,31)$.

Для этого нам понадобится следующее свойство индексов:

Свойство: *Два числа a_1 и a_2 сравнимы по простому модулю p тогда и только тогда, когда их индексы сравнимы по модулю $p-1$.*

$$a_1 \equiv a_2\,(mod\,p) \iff ind_\gamma\, a_1 \equiv ind_\gamma\, a_2\,(mod\,p-1).$$

Индексируем (по аналогии с логарифмированием) обе части сравнения.

$$ind\,15 + x \cdot ind\,21 \equiv ind\,19\,(\,mod\,30)$$

Мы воспользовались свойствами индексов, повторяющими известные свойства логарифмов. Подставим нужные индексы из таблицы и получим:

$$x \cdot 29 \equiv 4 - 21\,(\,mod\,30)$$

Решим сравнение первой степени

$$29x \equiv -17\,(\,mod\,30).$$

Для этого вспомним решение **задачи 13** или воспользуемся программой **Mathematica** .

input: **Reduce**[$29x == -17$, x, **Modulus** $\rightarrow$ **30**]
*(***Reduce** *решает уравнения и неравенства с двумя переменными, а также сравнения.* **Modulus** $\rightarrow$ **30** *задает область поиска неизвестной x, т.е. кольцо вычетов по модулю 30.)*

output: **17**
(Это ответ.)

1.13 Алгоритм шифрования Эль Гамаля

Задача. *Зашифровать и расшифровать сообщение* $M = 174$ *с помощью схемы шифрования Эль Гамаля (El Gamal).*

Даны простое число $P = 659$ *и число* $G = 409$. *Секретный ключ X и случайное число K требуется выбрать самостоятельно.*

Решение. Безопасность схемы Эль Гамаля, предложенной в 1985 году, основана на сложности вычисления дискретного логарифма в кольцах вычетов по большому простому модулю.

Простое число P и число $G < P$, данные в задаче не являются секретными и могут быть распространены среди группы пользователей. Число $X < P$ выбирается случайным образом и является секретным ключом. Пусть $X = 10$. Для шифрования сообщения M выбирается еще одно случайное число K, $1 < K < P - 1$, взаимно простое с $P - 1$. Поскольку $P - 1 = 658$, в качестве K можно взять 5.

Далее вычисляется открытый ключ Y:

$$Y = G^X (\, mod\, P) = 409^{10} (\, mod\, 659) = 471.$$

Несмотря на то, что показательное сравнение

$$G^X = Y (\, mod\, P)$$

известно всем, решить его, т.е. найти дискретный логарифм, практически невозможно [1] .

Затем вычисляем пару чисел (a, b), являющуюся шифртекстом для M:

$$a = G^K (\, mod\, P) = 409^5 (\, mod\, 659) = 347,$$

$$b = Y^K \cdot M (\, mod\, P) = 471^5 \cdot 174 (\, mod\, 659) =$$

[1] Для больших модулей P, которые имеют в двоичном представлении длину 512-1024 бит.

$$= 540 \cdot 174 (\, mod\, 659) = 382.$$

Итак $(a, b) = (347, 382)$.

Для расшифровывания шифртекста (a, b) надо вычислить

$$M = b \cdot (a^X)^{-1} (\, mod\, P),$$

т.е. решить сравнение первой степени

$$M \cdot a^X \equiv b (\, mod\, P).$$

В нашем случае

$$a^X (\, mod\, P) = 347^{10} (\, mod\, 659) = 540,$$

$$540^{-1} (\, mod\, 659) = 587,$$

$$M = 382 \cdot 587 (\, mod\, 659) = 174.$$

Глава 2

Индивидуальные задания по теории чисел

Задача 1. *Найти наибольший общий делитель (НОД) чисел a и b с помощью алгоритма Евклида. Представить НОД как линейную комбинацию чисел a и b (найти коэф-*

фициенты разложения $d = a \cdot u + b \cdot v$*).*

№	a	b	№	a	b
1	1760	2369	11	1950	2202
2	1935	2364	12	1657	2183
3	1503	2036	13	1657	2473
4	1646	2186	14	1679	2057
5	1957	2220	15	1763	2372
6	1899	2203	16	1645	2232
7	1927	2382	17	1676	2230
8	1824	2434	18	1899	2486
9	1719	2067	19	1623	2136
10	1883	2052	20	1936	2271

Задача 2. *Разложить число n на простые множители*
1) с помощью метода перебора простых делителей;
2) с помощью алгоритма Ферма.

№	n_1	n_2	№	n_1	n_2
1	289073200	19610627	11	11798800	19791743
2	365920	20035261	12	9780160	19678003
3	8416160	20091553	13	637760	19830253
4	9164480	19830253	14	193360	19779091
5	112280480	19526407	15	7878880	19838239
6	17347520	20014459	16	199875520	19787491
7	727360	19945931	17	10415600	19609873
8	86516800	19791743	18	8585440	19847621
9	2078960	19597661	19	8265920	19742267
10	4952480	19680839	20	43184800	19899361

Задача 3.

1. *Найти разложение рационального числа* $\frac{p}{q}$ *в непрерывную дробь, выписать подходящие дроби.*
2. *Найти разложение иррационального числа* x *в непрерывную дробь.*

№	p	q	x	№	p	q	x
1	1372	1168	$-2+2\sqrt{11}$	11	1220	1406	$-2+\sqrt{11}$
2	1242	1435	$2+2\sqrt{13}$	12	1057	1348	$1+\sqrt{7}$
3	1413	1358	$3+2\sqrt{7}$	13	1219	1175	$1+3\sqrt{5}$
4	1233	1074	$-3+2\sqrt{5}$	14	1351	1394	$-3+2\sqrt{13}$
5	1379	1428	$-2+3\sqrt{7}$	15	1194	1178	$3\sqrt{11}$
6	1442	1197	$-3+\sqrt{13}$	16	1151	1362	$-3+3\sqrt{13}$
7	1210	1089	$2+2\sqrt{5}$	17	1498	1145	$3+2\sqrt{5}$
8	1251	1205	$3+3\sqrt{13}$	18	1298	1191	$-1+\sqrt{11}$
9	1107	1440	$2\sqrt{11}$	19	1389	1408	$2\sqrt{7}$
10	1443	1239	$-3+2\sqrt{7}$	20	1446	1427	$-2+\sqrt{5}$

Задача 4. *Решить диофантово уравнение, используя подходящие дроби.*

1.	$130x + 210y = 20$	11.	$100x + 196y = 16$
2.	$180x + 210y = 90$	12.	$182x + 150y = 2$
3.	$168x + 130y = 8$	13.	$165x + 180y = 30$
4.	$130x + 169y = 13$	14.	$165x + 156y = 9$
5.	$180x + 156y = 24$	15.	$140x + 225y = 20$
6.	$140x + 110y = 30$	16.	$132x + 168y = 12$
7.	$132x + 182y = 8$	17.	$130x + 150y = 20$
8.	$156x + 110y = 2$	18.	$130x + 154y = 6$
9.	$225x + 121y = 2$	19.	$182x + 120y = 8$
10.	$156x + 195y = 117$	20.	$140x + 144y = 4$

Задача 5. *Найти остаток от деления степенного выражения a на число m.*

№	a	m	№	a	m
1.	3^{643}	7	11.	2^{748}	7
2.	2^{671}	8	12.	2^{776}	9
3.	5^{746}	9	13.	5^{728}	8
4.	4^{651}	8	14.	4^{708}	8
5.	2^{633}	8	15.	4^{624}	7
6.	4^{699}	9	16.	2^{611}	8
7.	5^{628}	8	17.	2^{754}	9
8.	5^{615}	8	18.	4^{710}	8
9.	3^{613}	9	19.	4^{684}	7
10.	2^{767}	7	20.	5^{761}	7

Задача 6. *Найти наименьшие положительные и наименьшие абсолютные вычеты по модулю m чисел:* $a_1, a_2, ..., a_n$. *Какие из этих чисел сравнимы по модулю m? Составить приведенную систему вычетов по модулю m.*

№	m	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9
1	19	6	13	32	−32	73	29	−20	131	132
2	19	7	12	31	−31	82	34	−24	152	153
3	19	10	9	28	−28	109	49	−36	215	216
4	15	4	11	26	−26	51	19	−12	89	90
5	12	4	8	20	−20	48	19	−12	89	90
6	16	7	9	25	−25	79	34	−24	152	153
7	16	8	8	24	−24	88	39	−28	173	174
8	17	7	10	27	−27	80	34	−24	152	153
9	16	5	11	27	−27	61	24	−16	110	111
10	12	9	3	15	−15	93	44	−32	194	195
11	14	8	6	20	−20	86	39	−28	173	174
12	17	4	13	30	−30	53	19	−12	89	90
13	17	8	9	26	−26	89	39	−28	173	174
14	15	3	12	27	−27	42	14	−8	68	69
15	19	4	15	34	−34	55	19	−12	89	90
16	11	7	4	15	−15	74	34	−24	152	153
17	14	4	10	24	−24	50	19	−12	89	90
18	13	7	6	19	−19	76	34	−24	152	153
19	15	5	10	25	−25	60	24	−16	110	111
20	12	10	2	14	−14	102	49	−36	215	216

Задача 7. *Вычислить значение функции Эйлера для чисел:* a_1, a_2, a_3.

№	a_1	a_2	a_3
1	9209	698167	151111737
2	8999	764107	345673783
3	9043	348091	8341659875
4	8647	424253	1511815019
5	8923	1161859	95175
6	9601	634507	69923697679
7	9463	1151627	7973721
8	8233	356309	10793861
9	8581	978251	186132037
10	9091	508163	23109625
11	7937	1144553	26773551
12	9413	1100401	1305640457
13	9491	1200127	432575
14	8609	835697	9657115625
15	9733	688549	1178455421
16	9043	363353	1273077
17	8219	684899	4440625
18	8599	867107	82820509373
19	8641	993227	2380862813
20	8747	891479	253333223

Задача 8. *Найти вычет, обратный к вычету* **a** *по модулю* **m***:*

1) *с помощью расширенного алгоритма Евклида;*

2) *с помощью теоремы Ферма.*

№	a_1	m_1	a_2	m_2	№	a_1	m_1	a_2	m_2
1	11	15	47	281	11	11	18	71	496
2	19	20	59	412	12	19	15	59	471
3	13	15	61	304	13	7	15	53	370
4	11	16	67	535	14	19	15	67	401
5	17	20	59	294	15	19	24	59	294
6	13	15	47	375	16	7	20	61	426
7	7	15	61	365	17	13	15	67	334
8	17	12	67	334	18	17	15	71	425
9	11	20	53	317	19	11	16	67	468
10	7	20	71	567	20	11	20	59	294

Задача 9. *Решить сравнение первой степени.*

1.	$41x \equiv 18\,(mod\,53)$	11.	$48x \equiv 10\,(mod\,49)$
2.	$62x \equiv 17\,(mod\,63)$	12.	$39x \equiv 10\,(mod\,34)$
3.	$37x \equiv 18\,(mod\,54)$	13.	$53x \equiv 16\,(mod\,67)$
4.	$46x \equiv 15\,(mod\,47)$	14.	$35x \equiv 15\,(mod\,57)$
5.	$47x \equiv 13\,(mod\,52)$	15.	$49x \equiv 10\,(mod\,64)$
6.	$56x \equiv 17\,(mod\,55)$	16.	$44x \equiv 17\,(mod\,49)$
7.	$57x \equiv 10\,(mod\,44)$	17.	$55x \equiv 17\,(mod\,38)$
8.	$62x \equiv 13\,(mod\,63)$	18.	$40x \equiv 16\,(mod\,41)$
9.	$55x \equiv 16\,(mod\,34)$	19.	$65x \equiv 17\,(mod\,66)$
10.	$58x \equiv 18\,(mod\,45)$	20.	$57x \equiv 10\,(mod\,49)$

Задача 10. *Решить систему сравнений первой степени с помощью китайской теоремы об остатках.*

$$\begin{cases} x \equiv a_1 (mod\, m_1) \\ x \equiv a_2 (mod\, m_2) \\ x \equiv a_3 (mod\, m_3) \end{cases}$$

№	a_1	a_2	a_3	m_1	m_2	m_3	№	a_1	a_2	a_3	m_1	m_2	m_3
1	20	36	23	11	31	71	11	10	33	32	17	31	67
2	11	31	10	13	43	53	12	30	18	18	17	31	71
3	24	18	30	29	41	59	13	40	35	21	23	47	71
4	11	14	29	7	37	71	14	31	16	19	19	41	53
5	13	14	28	23	41	61	15	37	28	27	23	41	67
6	26	18	35	11	37	61	16	23	24	35	7	47	71
7	21	12	29	11	37	61	17	38	15	35	11	41	67
8	22	31	27	23	37	59	18	12	12	39	19	37	61
9	32	34	17	23	43	59	19	30	22	26	17	47	59
10	27	14	32	23	43	53	20	22	31	30	7	31	59

Задача 11. *Зашифровать и расшифровать сообщение с помощью криптосистемы RSA (R. Rivest, A. Shamir, L. Adleman). Даны простые числа p и q (закрытая часть ключа) и сообщение M. Требуется выбрать вторую часть открытого ключа e,построить третью часть закрытого ключа d, зашифровать и расшифровать сообщение M.*

№	p	q	M	№	p	q	M
1.	233	353	25	11.	283	419	30
2.	239	359	22	12.	293	421	30
3.	241	367	21	13.	307	431	26
4.	251	373	21	14.	311	433	26
5.	257	379	29	15.	313	439	27
6.	263	383	28	16.	317	443	30
7.	269	389	24	17.	331	449	29
8.	271	397	23	18.	337	457	27
9.	277	401	27	19.	347	461	24
10.	281	409	27	20.	349	463	29

Задача 12. *1) Для простого модуля* ***m*** *найти первообразный корень и составить таблицу индексов для приведенной системы вычетов по модулю* ***m****.*
2) С помощью таблицы индексов решить сравнение $a \cdot b^x \equiv c\,(mod\, m)$

№	**a**	**b**	**c**	**m**	№	**a**	**b**	**c**	**m**
1	18	51	20	53	11	21	59	18	61
2	20	57	20	59	12	13	57	17	59
3	20	65	21	67	13	22	45	22	47
4	13	41	9	43	14	23	57	7	59
5	17	27	26	29	15	8	51	16	53
6	7	41	8	43	16	26	27	12	29
7	25	15	19	17	17	7	29	14	37
8	14	51	14	53	18	22	51	26	53
9	21	59	12	61	19	20	21	16	23
10	27	27	22	29	20	17	57	23	59

Задача 13. *Зашифровать и расшифровать сообщение* ***M*** *с помощью схемы шифрования Эль Гамаля (El Gamal). Даны простое число* ***P*** *и число* ***G****. Секретный ключ* ***X*** *и случайное число* ***K*** *требуется выбрать самостоятельно.*

№	P	G	M	№	P	G	M
1	661	434	115	11	1063	495	105
2	653	453	147	12	563	456	118
3	617	464	133	13	1039	443	158
4	1109	437	120	14	1187	463	111
5	919	416	120	15	641	406	199
6	599	412	185	16	997	493	141
7	769	433	112	17	719	440	142
8	977	450	199	18	1069	430	198
9	751	436	192	19	691	484	134
10	613	470	186	20	733	451	138

Приложение 1.

Простые числа $p < 100$, их наименьшие первообразные корни γ и таблицы индексов.

$p = 3$, $\gamma = 2$

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

$p = 5$, $\gamma = 2$

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

$p = 7$, $\gamma = 3$

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

$p = 11$, $\gamma = 2$

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

$p = 13$, $\gamma = 2$

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	–	–	–	–	–	–	–	–

$p = 17$, $\gamma = 3$

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	–	–	–	–

$p = 19$, $\gamma = 2$

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	–	–

$p = 23$, $\gamma = 5$

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	–	–	–	–	–	–	–	–

$p = 29$, $\gamma = 2$

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	–	–

$p = 31$, $\gamma = 3$

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
3	–	–	–	–	–	–	–	–	–	–

$p = 37$, $\gamma = 2$

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	–	–	–	–

$p = 41$, $\gamma = 6$

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
4	–	–	–	–	–	–	–	–	–	–

$p = 43$, $\gamma = 3$

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	–	–	–	–	–	–	–	–

$p = 47$, $\gamma = 5$

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	–	–	–	–

$p = 53$, $\gamma = 2$

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	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	–	–	–	–	–	–	–	–

$p = 59$, $\gamma = 2$

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	–	–

$p = 61$, $\gamma = 2$

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	–	–	–	–	–	–	–	–	–	–

$p = 67$, $\gamma = 2$

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	–	–	–	–

$p = 71$, $\gamma = 7$

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	–	–	–	–	–	–	–	–	–	–

$p = 73$, $\gamma = 5$

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	–	–	–	–	–	–	–	–

$p = 79$, $\gamma = 3$

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	–	–

$p = 83$, $\gamma = 2$

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	18	36	72	61	39	78	73
7	63	43	3	6	12	24	48	13	26	52
8	21	42	–	–	–	–	–	–	–	–

$p = 89$, $\gamma = 3$

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	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	–	–

$p = 97$, $\gamma = 5$

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	–	–	–	–

Приложение 2.

Функции программы Mathematica, полезные при решении задач теории чисел.

1. Чтобы проверить, делит ли целое d целое число n, можно использовать функцию IntegerQ. Например,
   IntegerQ[34]
   True

2. Функция Divisors дает список всех натуральных делителей числа n. Например,
   Divisors[12345]
   {1, 3, 5, 15, 823, 2469, 4115, 12345}

3. Функция Prime[k] выдает k-е простое число. Например,
   Prime[23]
   83

4. Функция PrimeQ[n] проверяет простоту числа n. Например,
   PrimeQ[34567]
   False

5. Функция $\pi(n)$ подсчитывает число простых чисел, не превосходящих n. В пакете "Mathematica"эта функция обозначается PrimePi [n].
   PrimePi[123]
   False

6. НОД(a, b) — наибольшее целое число, делящее как a, так и b.

НОК(a, b) — наименьшее натуральное число, делящееся на a и b.

В пакете "Mathematica"имеются соответствующие функции GCDи LCM:

GCD[123, 456]

3

LCM[123, 456]

18696

7. Функция FactorInteger[n] дает разложение целого числа n. Выходом служит список пар. Каждая пара содержит простой делитель числа n и его показатель.

   FactorInteger[123456789]

   {{3, 2}, {3607, 1}, {3803, 1}}

   a = 21375; b = 89775;

   FactorInteger[a]

   FactorInteger[b]

   FactorInteger[GCD[a, b]]

   FactorInteger[LCM[a, b]]

   GCD[a, b]*LCM[a, b] == a*b

   {{3, 2}, {5, 3}, {19, 1}}

   {{3, 3}, {5, 2}, {7, 1}, {19, 1}}

   {{3, 2}, {5, 2}, {19, 1}}

   {{3, 3}, {5, 3}, {7, 1}, {19, 1}}

   True

8. ExtendedGCD – расширенная версия алгоритма Евклида.

   ExtendedGCD[1645, 861]

   {7, {-56, 107}}

9. Функция Mod[a, n] из пакета "Mathematica"дает единственное целое $r, 0 < r < n$, такое, что $a \equiv r(mod\, n)$.
   Mod[12345, 13]
   8

10. Следующий пример показывает, как легко проверить сравнимость двух целых чисел по модулю *m*:
    m = 13; a = 12345; b = 103579; Mod[a - b, m] == 0
    True

11. Чтобы вычислить в "Mathematica"непрерывную дробь числа, нужно сначала загрузить пакет NumberTheory'ContinuedFractions'.
    « NumberTheory'ContinuedFractions'

12. Для нахождения непрерывной дроби рационального числа можно использовать функцию ContinuedFraction.
    ContinuedFraction[135 / 159]

$$0 + \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2}}}}}}$$

13. Если α не рационально, можно указать желаемое число этажей непрерывной дроби.

ContinuedFraction[Pi, 11]

$$3+\cfrac{1}{7+\cfrac{1}{15+\cfrac{1}{1+\cfrac{1}{292+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\frac{1}{3}}}}}}}}}}$$

14. Чтобы выразить непрерывную дробь обычной дробью, можно воспользоваться функцией Normal.
Normal[ContinuedFraction[Pi, 11]]
$\frac{4272943}{1360120}$

15. Если непрерывная дробь задана в виде $[a_0, a_1, ..., a_m]$, то обычную непрерывную дробь можно получить с помощью функции ContinuedFractionForm.
AA = {3, 7, 15, 1, 292} ContinuedFractionForm[AA]

16. Функция Эйлера определяется равенством $\varphi(m) = \{i$: $0 < i < m$, НОД$(i,m) = 1\}$. Иными словами, $\varphi(m)$ — это число целых чисел между 0 и $m - 1$, которые взаим-

но просты с m. В пакете "Mathematica"этой функции отвечает EulerPhi. Например,

m = 15; EulerPhi[m]

8

17. Возведение в степень по модулю некоторого целого числа в пакете "Mathematica"может выполняться много быстрее с помощью функции PowerMod, которая приводит все промежуточные результаты при вычислении a^b по модулю n.

    m = 123456789; a = 1111111111; GCD[m, a]
    PowerMod[a, EulerPhi[m], m]

    1

    1

18. Чтобы решить сравнения $x \equiv b_i (mod\, m_i), 1 < i < k$, где все m_i взаимно просты, с помощью китайской теоремы об остатках в системе "Mathematica нужно сначала загрузить пакет NumberTheory'NumberTheoryFunctions'.

    « NumberTheory'NumberTheoryFunctions'

19. Теперь систему сравнений можно решить с помощью функции ChineseRemainderTheorem.

ЛИТЕРАТУРА

1. Виноградов, И. М. Основы теории чисел — Москва : Издательство Юрайт, 2023.

2. Дэвенпорт Г. Введение в теорию чисел — Вузовская книга, 2008.

3. Нестеренко, Ю.В. Теория чисел — Издательство: М.: Академия, 2008.

4. Айерленд К., Роузен М. Классическое ведение в современную теорию чисел. — М.: Мир, 1987.

5. Новиков Ф.А. Дискретная математика для программистов. — СПб: Питер, 2000.

6. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. — М.: Постмаркет, 2001.

7. Акритас А. Основы компьютерной алгебры с приложениями. — М. Мир, 1994.

8. Фергюнсон Н., Шнайдер Б. Практическая криптография. — М.: Издательский дом "Вильямс 2005.

9. Дьяконов В.П. Mathematica 5.1/5.2/6.0. Программирование и математические вычисления. — М.: ДМК пресс, 2008.

Оглавление

Учебное издание

Ю.Б. Ржонсницкая,
И.В. Зайцева,
Е.А. Бровкина

ОСНОВЫ ТЕОРИИ ЧИСЕЛ

Печатается в авторской редакции.

Подписано в печать 30.12.2022. Формат 60×90 1/16.
Гарнитура Times New Roman. Печать цифровая.
Усл. печ. л. 5,25. Тираж 10 экз. Заказ № 1339.
РГГМУ, 192007, Санкт-Петербург, Воронежская ул., д. 79.