РЕШЕНИЯ (ЗАПАД)

Решение 1.

Сначала заметим, что если $N = pq$, где p и q – простые числа, количество натуральных чисел, меньших N и взаимно простых с N равно $(p-1)(q-1)$ (обозначим это число как $\varphi(N)$). Это можно понять, если составить таблицу, содержащую p строк и q столбцов

	1	2	…	$q-1$	q
1	+	+	…	+	–
2	+	+	…	+	–
⋮	⋮	⋮	⋮	⋮	⋮
$p-1$	+	+	…	+	–
p	–	–		–	–

в ячейках которой значком “–” отмечать те числа вида $t_1 \cdot t_2,\ t_1 \in \{1,...,p\}, t_2 \in \{1,...,q\}$, которые содержат с $\varphi(N)$ общие сомножители, а “+” – которые не содержат.

Поэтому, получаем систему: $\begin{cases} pq = N \\ (p-1)(q-1) = \varphi(N) \end{cases}$; $\begin{cases} pq = N \\ p+q = N+1-\varphi(N) \end{cases}$.

По теореме Виета получаем, что p и q – решения квадратного уравнения:

$$x^2 - (N+1-\varphi(N))x + N = 0.$$

В представленной задаче $N = 203060593$, $\varphi(N) = 203030388$ и квадратное уравнение примет вид:

$$x^2 - 30206x + 203060593 = 0.$$

Тогда:

$$\sqrt{D} = \sqrt{100160064}.$$

Для того, чтобы извлечь квадратный корень из этого числа можно заметить, что результат должен быть немного больше, чем 10000, причем последняя цифра в этом числе должны быть 2 или 8. Тогда претендентами будут следующие числа: 10002, 10008, 10012, 10018… Начинаем последовательно возводить их в квадрат, в результате находим: $10008^2 = 100160064$. Итак:

$$x_1 = \frac{30206-10008}{2} = 10099 = p;$$

$$x_2 = \frac{30206+10008}{2} = 20107 = q.$$

ОТВЕТ: 10099 и 20107.

Решение 5.

Фактически надо найти x,y такие, что $ax + by = n$. Уравнение $ax + by = n$, в котором НОД(a,b)=1, неразрешимо в неотрицательных целых числах x, y при $n = F(a,b) = ab - a - b$ и разрешимо при всех натуральных $n > F(a,b) = ab - a - b$. Число *F(a,b)* называется числом Фробениуса для пары *(a,b)*. В самом деле, покажем, что уравнение $ax + by = c$ не имеет натуральных решений *x, y* при $c = ab$ и имеет такие решения при всех $c > ab$. Пусть при натуральных *a, b, x, y* выполнено $ax + by = ab$, тогда $ax = b(a-y)$, т.е. *x* делится на *b*, откуда $x \ge b$, тогда $ax + by > ab$. Пусть *c>ab* тогда в силу НОД(*a,b*)=1 найдутся такие натуральные *u,v*, что $au - bv = c > ab$, т.е. $\frac{u}{b} - \frac{v}{a} > 1$.

Следовательно, найдется такое натуральное *t*, что $\frac{u}{b} > t > \frac{v}{a}$. При этом t зададим натуральные числа $x = u - bt, y = at - v$. Тогда

$$ax + by = a(u-bt) + b(at-v) = au - bv = c.$$

Перебором чисел от 1 до 23 находим не возможные значения. Любое значение 24 и более возможно.

ОТВЕТ: {4,8,9,12,13,16,17,18, 20, 21, 22, 24, далее все}

Решение 2.

Пусть в двоичной системе координат $A = (x_n,...,x_0)$. Тогда $A_1 = (x_3, x_2, x_1, x_0)$, $A_2 = (x_4, x_3, x_2, x_1)$, $A_3 = (x_5, x_4, x_3, x_2)$. Следовательно,

$a_1 \oplus a_2 = (A_1 \oplus B) \oplus (A_2 \oplus B) = A_1 \oplus A_2 = (x_3 \oplus x_4, x_2 \oplus x_3, x_1 \oplus x_2, x_0 \oplus x_1)$,

$a_3 \oplus a_2 = (A_3 \oplus B) \oplus (A_2 \oplus B) = A_3 \oplus A_2 = (x_5 \oplus x_4, x_4 \oplus x_3, x_3 \oplus x_2, x_2 \oplus x_1)$.

Итак, если вычислить $a_1 \oplus a_2$, то три младших бита $a_3 \oplus a_2$ будут найдены, а старший бит будет произвольным.

Вычислим значение $a_1 \oplus a_2$:

$$\begin{array}{cccc} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ \hline 1 & 1 & 0 & 0 \end{array}$$

РЕШЕНИЯ (ЗАПАД)

Решение 2 (продолжение).

Тогда возможные значения $a_3 \oplus a_2$ имеют вид $(*,1,1,0)$, и $a_3 = a_2 \oplus (a_3 \oplus a_2)$:

```
1 0 1 0
* 1 1 0
-------
* 1 0 0
```

ОТВЕТ: 12 и 4.

Решение 3.

Одно из возможных решений указано в таблице:

№ хода	Вариант Юры
1.	0 0 0 0
2.	0 0 0 1
3.	0 0 1 1
4.	0 0 1 0
5.	0 1 1 0
6.	0 1 1 1
7.	0 1 0 1
8.	0 1 0 0
9.	1 1 0 0
10.	1 1 0 1
11.	1 1 1 1
12.	1 1 1 0
13.	1 0 1 0
14.	1 0 1 1
15.	1 0 0 1
16.	1 0 0 0

Юра для гарантированного выигрыша должен начать с комбинации «0000» и потом за следующие 15 шагов перечислить все комбинации, причем следующая комбинация должна отличаться от предыдущей только в одной позиции.

Решение 4.

Способ 1. «Протягиваем» указанное в условии слово по шифрованному тексту. При правильном расположении после вычитания слова из фрагмента шифрованного текста получим значения, образующие геометрическую прогрессию по модулю 31.

…	Щ	Ж	Ч	Ф	Х	С	Ч	…
	З	О	Л	О	Т	А	Я	
…	25	7	23	20	21	17	23	…
…	8	14	11	14	19	0	30	…
…	17	24	12	6	3	17	7	…

Способ 2. Заметим, что каждая геометрическая прогрессия указанного вида получается умножением цикла 1,2,4,8,16,1 на константу и/или регулярной выборкой с шагом 2,3,4 из нее – в зависимости от значений параметров a и b. Т.о. период каждой прогрессии указанного вида равен 5.

В слове ЗОЛОТАЯ первая буква (8) и шестая буква (0) различаются на 8. Ищем в шифрованном тексте разнесенные на расстояние 5 буквы, отстоящие по алфавиту на 8 одна от другой. Далее вычитаем слово из фрагмента шифртекста, пользуясь периодичностью, продолжаем вправо и влево шифрующую последовательность и находим исходный текст.

Щ	Ж	Ч	Ф	Х	С	Ч
З	О	Л	О	Т	А	Я
25	7	23	20	21	17	23
8	14	11	14	19	0	30
17	24	12	6	3	17	7

ОТВЕТ:

ОТГОВОРИЛАРОЩА**ЗОЛОТАЯ**БЕРЕЗОВЫМВЕСЕЛЫМЯЗЫКОМ

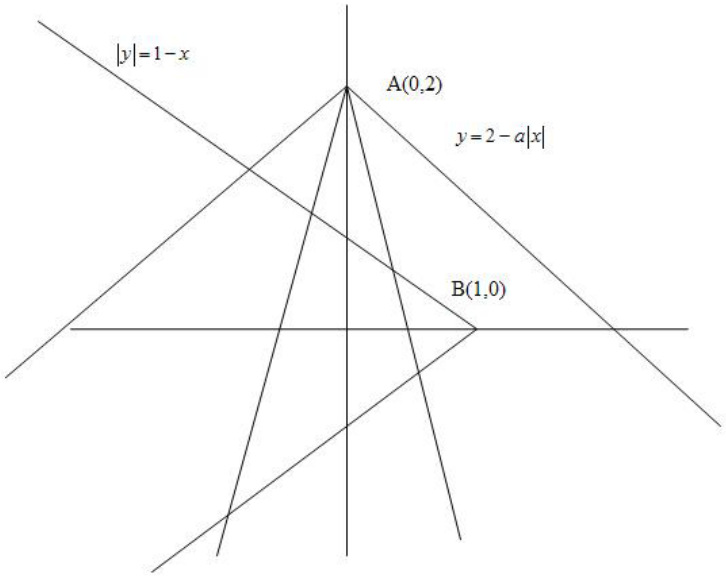
b=24, a=4, период равен 5.

Решение 6.

Приведем геометрическое решение данной задачи.

а) Рассмотрим графики линий, задаваемых системой уравнений при $a>0$:

$$\begin{cases} |y| = 1-x \\ y = 2-a|x| \end{cases}$$



Отсюда видно, что при $a>0$ система может иметь 1, 2, 3 или 4 решения.

Ровно 3 решения система имеет при тех $a>0$, при которых луч $y=2-ax,\quad x>0$ проходит через точку $B(1,0)$, то есть при $a=2$.

При $a>2$ луч $y=2-ax,\quad x>0$ пересекает линию $|y|=1-x$ в двух точках. Поэтому в данном случае система имеет ровно 4 решения.

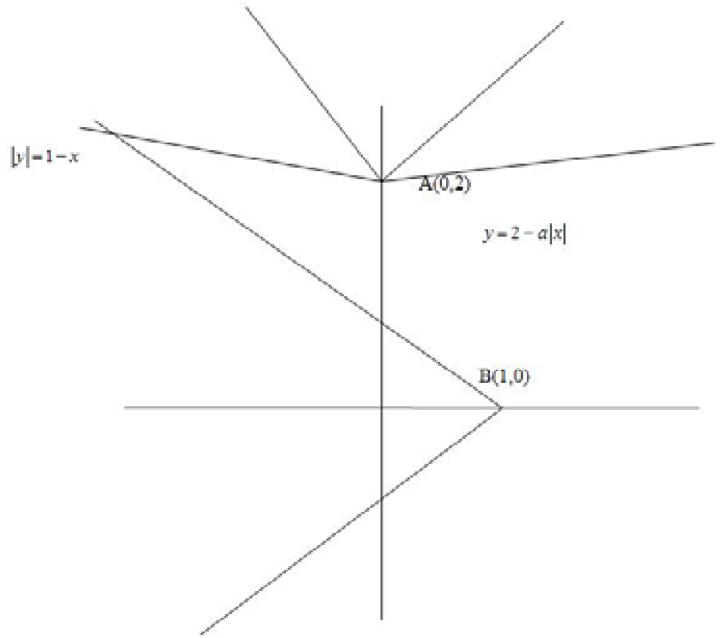
При $0<a<2$ луч $y=2-ax,\quad x>0$ не пересекает линию $|y|=1-x$. Поэтому в данном случае система имеет 1 или 2 решения. Два решения получаются пересечением луча $y=2-a|x|,\quad x<0$ и линии $|y|=1-x$ в двух точках. Это может быть, если луч $y=2-a|x|,\quad x<0$ имеет угловой коэффициент (который равен a) больший, чем 1.

Итак, при $1<a<2$ система имеет ровно 2 решения.

Если же $0<a\le 1$, то система имеет 1 решение.

Решение 6 (продолжение).

б) Рассмотрим графики линий, задаваемых системой уравнений при $a<0$:



Отсюда видно, что при $a<0$ система может иметь 0 или 1 решение.

Система не имеет решений при тех $a<0$, при которых луч $y=2-a|x|,\quad x<0$ не пересекает линию $|y|=1-x$, то есть при $a\le -1$.

При $-1<a<0$ луч $y=2-a|x|,\quad x<0$ пересекает линию $|y|=1-x$ ровно в 1 точке. Поэтому в данном случае система имеет ровно 1 решение.

в) При $a=0$ система, очевидно, имеет ровно 1 решение $(-1;2)$

ОТВЕТ:

- при $a\le -1$ нет решений;
- при $-1<a\le 1$ система имеет 1 решение;
- при $1<a<2$ система имеет 2 решения;
- при $a=2$ система имеет 3 решения;
- при $a>2$ система имеет 4 решения.

XIX
МЕЖРЕГИОНАЛЬНАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО МАТЕМАТИКЕ И КРИПТОГРАФИИ
РЕШЕНИЯ (ЗАПАД)

11 КЛАСС
ВАРИАНТ 2

Решение 1.

Сначала заметим, что если $N = pq$, где p и q – простые числа, количество натуральных чисел, меньших N и взаимно простых с N равно $(p-1)(q-1)$ (обозначим это число как $\varphi(N)$). Это можно понять, если составить таблицу, содержащую p строк и q столбцов

	1	2	…	$q-1$	q
1	+	+	…	+	–
2	+	+	…	+	–
⋮	⋮	⋮	⋮	⋮	⋮
$p-1$	+	+	…	+	–
p	–	–		–	–

в ячейках которой значком “–” отмечать те числа вида $t_1 \cdot t_2,\ t_1 \in \{1,...,p\},\ t_2 \in \{1,...,q\}$, которые содержат с $\varphi(N)$ общие сомножители, а “+” – которые не содержат.

Поэтому, получаем систему: $\begin{cases} pq = N \\ (p-1)(q-1) = \varphi(N) \end{cases}$; $\begin{cases} pq = N \\ p+q = N+1-\varphi(N) \end{cases}$.

По теореме Виета получаем, что p и q – решения квадратного уравнения:

$$x^2 - (N+1-\varphi(N))x + N = 0.$$

В представленной задаче $N = 202718099$, $\varphi(N) = 202687920$ и квадратное уравнение примет вид:

$$x^2 - 30180x + 202718099 = 0.$$

Тогда:

$$\sqrt{D} = \sqrt{99960004}.$$

Для того, чтобы извлечь квадратный корень из этого числа можно заметить, что результат должен быть немного меньше, чем 10000, причем последняя цифра в этом числе должны быть 2 или 8. Тогда претендентами будут следующие числа: 9998, 9992, 9988, 9982… Начинаем последовательно возводить их в квадрат, в результате находим: $9998^2 = 99960004$. Итак:

$$x_1 = \frac{30180 - 9998}{2} = 10091 = p;$$

$$x_2 = \frac{30180 + 9998}{2} = 20089 = q.$$

ОТВЕТ: 10091 и 20089.

Решение 5.

Фактически надо найти x,y такие, что $ax + by = n$. Уравнение $ax + by = n$, в котором НОД(a,b)=1, неразрешимо в неотрицательных целых числах *x, y* при $n = F(a,b) = ab - a - b$ и разрешимо при всех натуральных $n > F(a,b) = ab - a - b$. Число *F(a,b)* называется числом Фробениуса для пары *(a,b)*. В самом деле, покажем, что уравнение $ax + by = c$ не имеет натуральных решений *x, y* при $c = ab$ и имеет такие решения при всех $c > ab$. Пусть при натуральных *a, b, x, y* выполнено $ax + by = ab$, тогда $ax = b(a-y)$, т.е. *x* делится на *b*, откуда $x \ge b$, тогда $ax + by > ab$. Пусть *c*>*ab* тогда в силу НОД(a,b)=1 найдутся такие натуральные *u*,*v*, что $au - bv = c > ab$, т.е. $\frac{u}{b} - \frac{v}{a} > 1$.

Следовательно, найдется такое натуральное *t*, что $\frac{u}{b} > t > \frac{v}{a}$.При этом t зададим натуральные числа $x = u - bt,\ y = at - v$. Тогда

$$ax + by = a(u - bt) + b(at - v) = au - bv = c.$$

Перебором чисел от 1 до 17 находим не возможные значения. Любое значение 18 и более возможно.

ОТВЕТ: {3,6,9,10,12,13,15,16,18 далее все}

Решение 2.

Пусть в двоичной системе координат $A = (x_n, ..., x_0)$. Тогда $A_1 = (x_3, x_2, x_1, x_0)$, $A_2 = (x_4, x_3, x_2, x_1)$, $A_3 = (x_5, x_4, x_3, x_2)$. Следовательно,

$a_1 \oplus a_2 = (A_1 \oplus B) \oplus (A_2 \oplus B) = A_1 \oplus A_2 = (x_3 \oplus x_4, x_2 \oplus x_3, x_1 \oplus x_2, x_0 \oplus x_1)$,

$a_3 \oplus a_2 = (A_3 \oplus B) \oplus (A_2 \oplus B) = A_3 \oplus A_2 = (x_5 \oplus x_4, x_4 \oplus x_3, x_3 \oplus x_2, x_2 \oplus x_1)$.

Итак, если вычислить $a_1 \oplus a_2$, то три младших бита $a_3 \oplus a_2$ будут найдены, а старший бит будет произвольным.

Вычислим значение $a_1 \oplus a_2$:

$$\begin{array}{cccc} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ \hline 0 & 0 & 1 & 0 \end{array}.$$

РЕШЕНИЯ (ЗАПАД)

Решение 2 (продолжение).

Тогда возможные значения $a_3 \oplus a_2$ имеют вид $(*,0,0,1)$, и $a_3 = a_2 \oplus (a_3 \oplus a_2)$:

```
1 0 1 1
* 0 0 1
-------
* 0 1 0
```

ОТВЕТ: 10 и 2.

Решение 3.

Одно из возможных решений указано в таблице:

№ поездки	К Ж З
1	0 0 1
2	0 1 1
3	0 1 0
4	1 1 0
5	1 1 1
6	1 0 1
7	1 0 0
8	0 0 0

Названия станций заменяются комбинациями нулей и единиц, в которых единицами отмечается присутствие в названии соответствующего цвета. Номеру поездки соответствует станция прибытия. Для того, чтобы такая таблица соответствовала решению, все комбинации должны быть перечислены и последовательные комбинации должны отличаться в одном разряде.

Решение 4.

Способ 1. «Протягиваем» указанное в условии слово по шифрованному тексту. При правильном расположении после вычитания слова из фрагмента шифрованного текста получим значения, образующие геометрическую прогрессию по модулю 31.

…	Е	Б	Т	Н	З	Ё	Д	…
	Г	Р	О	М	А	Д	У	
…	5	1	18	13	8	6	4	…
…	3	16	14	12	0	4	19	…
…	2	16	4	1	8	2	16	…

Способ 2. Заметим, что каждая геометрическая прогрессия указанного вида получается умножением цикла 1,2,4,8,16,1 на константу и/или регулярной выборкой с шагом 2,3,4 из нее – в зависимости от значений параметров a и b. Т.о. период каждой прогрессии указанного вида равен 5.

В слове ГРОМАДУ первая (3) и шестая буквы (4) идут подряд в алфавите. Ищем в шифрованном тексте разнесенные на расстояние 5 буквы, отстоящие по алфавиту на 1 одна от другой. Далее вычитаем слово из фрагмента шифртекста, пользуясь периодичностью, продолжаем вправо и влево шифрующую последовательность и находим исходный текст.

Е	Б	Т	Н	З	Ё	Д
Г	Р	О	М	А	Д	У
5	1	18	13	8	6	4
3	16	14	12	0	4	19
2	16	4	1	8	2	16

ОТВЕТ:

МОЙСТИХТРУДОМ**ГРОМАДУ**ЛЕТПРОРВЕТИЯВИТСЯВЕСОМОГРУБОЗРИМО

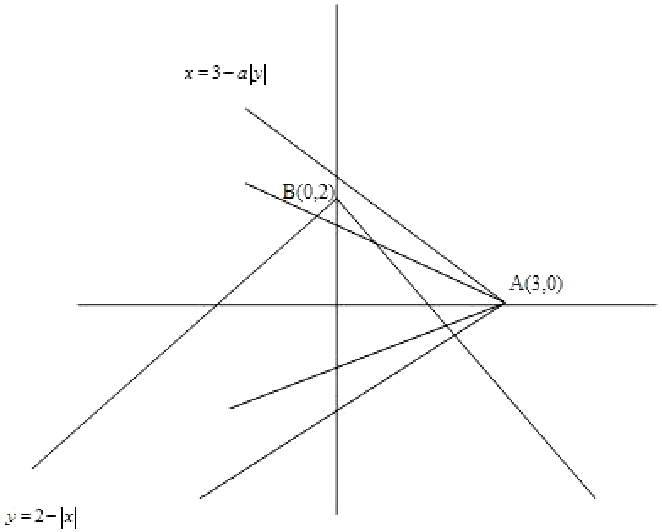
b=4, a=3, период равен 5.

Решение 6.

Приведем геометрическое решение данной задачи.

а) Рассмотрим графики линий, задаваемых системой уравнений при $a>0$:

$$\begin{cases} y=2-|x| \\ x=3-a|y| \end{cases}$$



Отсюда видно, что при $a>0$ система может иметь 1, 2, 3 или 4 решения.

Ровно 3 решения система имеет при тех $a>0$, при которых луч $x=3-ay$, $y>0$ проходит через точку $B(0,2)$, то есть при $a=1{,}5$.

При $a>1.5$ луч $x=3-ay$, $y>0$ пересекает линию $y=2-|x|$ в двух точках. Поэтому в данном случае система имеет ровно 4 решения.

При $0<a<1.5$ луч $x=3-ay$, $y>0$ не пересекает линию $y=2-|x|$. Поэтому в данном случае система имеет 1 или 2 решения. Два решения получаются пересечением луча $x=3-a|y|$, $y<0$ и линии $y=2-|x|$ в двух точках. Это может быть, если луч $x=3-a|y|$, $y<0$ имеет угловой коэффициент (который равен $\frac{1}{a}$) меньший, чем 1.

Итак, при $1<a<1.5$ система имеет ровно 2 решения.

Если же $0<a\le 1$, то система имеет 1 решение.

Решение 6 (продолжение).

б) Рассмотрим графики линий, задаваемых системой уравнений при $a<0$:

Отсюда видно, что при $a<0$ система может иметь 0 или 1 решение. Система не имеет решений при тех $a<0$, при которых луч $x=3-a|y|$, $y<0$ не пересекает линию $y=2-|x|$, то есть при $-1\le\frac{1}{a}<0$ (точнее при $a\le -1$). При $-1<a<0$ луч $x=3-a|y|$, $y<0$ пересекает линию $y=2-|x|$ ровно в 1 точке. Поэтому в данном случае система имеет ровно 1 решение.

в) При $a=0$ система, очевидно, имеет ровно 1 решение $(3;-1)$

ОТВЕТ:

- при $a\le -1$ нет решений;
- при $-1<a\le 1$ система имеет 1 решение;
- при $1<a<1.5$ система имеет 2 решения;
- при $a=1{,}5$ система имеет 3 решения;
- при $a>1.5$ система имеет 4 решения.