Решение олимпиады ФПМИ 2020

9 –10 классы

1. Инверсией в перестановке P длины n называется любая пара индексов i,j такая, что 1 <= i < j <= n и P_i > P_j. Четностью перестановки называется четность числа инверсий в ней. Факт: Количество различных перестановок длины n - n!. Докажите это самостоятельно.

   Докажем следующий факт: операция транспозиции меняет четность перестановки. Рассмотрим транспозицию меняющую местами элементы на позициях i, j. Так как все элементы кроме i, j остались на своих позициях, то инверсии могли появиться или пропасть только с i-ым или j-ым элементами. Будем рассматривать только пары индексов {i, k} и {j, k}. Тогда для всех 1 <= k < i и для всех n >= k > j количество инверсий не изменилось (т.к. порядок {k,i} и {k,j} в перестановке остался прежним). Для i < k < j обе пары {i, k}, {k, j} либо станут инверсией либо перестанут ей быть, следовательно четность количества инверсий в перестановке не изменится. И еще пара {i, j} либо станет инверсией либо перестанет ей быть, следовательно четность перестановки изменится.

   Факт: Набор из всех четных перестановок удовлетворяет условию задачи. Действительно, для любых двух перестановок P, Q из этого набора нельзя получить P из Q за одну транспозицию т.к. у них одинаковая четность.

   Факт: Количество четных перестановок длины n - n!/2. Для каждой нечетной перестановки P поставим в пару перестановку получающуюся транспозицией первого и второго элементов перестановки. Тогда во всех парах будут четная и нечетные перестановки, притом в разных парах будут разные перестановки. Из этого следует, что число четных перестановок равно числу нечетных и равно n!/2. Также из этого следует, что если выбрать более n!/2 перестановок, то какие-то две выбранные перестановки будут из одной пары, а следовательно будут достижимы из друг друга одной операцией транспозиции. Значит мы построили пример состоящий из n!/2 перестановок удовлетворяющих условию задачи, а также доказали что примера большего размера нет.

   Задача решена, ответ n!/2.

2. Покажем, что если число *x* будет решением уравнения, то и число 2020-*x* также будет решением.

$$[(2020-x)^2]+a-2020(2020-x)=$$
$$=[2020^2-4040x+x^2]+a-2020^2+2020x=$$
$$=[-4040x+x^2]+a+2020x=*$$

Заметим, что поскольку x – корень уравнения, то $4040x = 2[x^2] + 2a$.

$$* = [-2[x^2] - 2a + x^2] + a + 2020x = -2[x^2] - 2a + [x^2] + a + 2020x = $$
$$= -[x^2] - a + 2020x = 0.$$

Соответственно, для того, чтобы корней было нечетное количество необходимо, чтобы выполнялось равенство $2020 - x = x$. Т.е. $x = 1010$. Тогда $a = 1010^2$. Решим уравнение при данном значении параметра. Заметим, что поскольку справа стоит целое число, то слева также будет целое. Значит, по определению целой части выполняется двойное неравенство

$$2020x - 1010^2 \leq x^2 < 2020x - 1010^2 + 1.$$

Отсюда получаем

$$0 \leq (x - 1010)^2 < 1.$$

Следовательно решением уравнения будут являться все числа $1010 + p$, где $-1 < p < 1$. Причем $2020p$ – целое число.

Ответ: $a = 1010^2$. Ни при каких целых значениях параметра a уравнение не может иметь единственного решения.

3. Заметим, что при любых натуральных значениях x числа x и $f(x)$ взаимно просты. Соответственно если выполнено условие $f(k)\ f(l)$ делится на kl, то $f(k)$ делится на l, а $f(l)$ делится на k. Учитывая все три условия получим, что $f(k)$ делится на l и m, $f(l)$ делится на k и m, $f(m)$ делится на k и l.

Кроме того, заметим, что числа k, l, m попарно взаимно просты. Действительно, если НОД(k, l)=d, то $f(k)$ делится на d. А это противоречит взаимной простоте чисел k и $f(k)$.

Из последнего утверждения следует, что $f(k)$ делится на lm, $f(l)$ делится на km, $f(m)$ делится на kl.

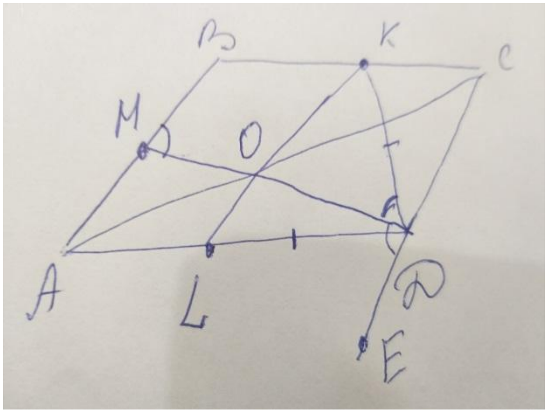
Пусть k наименьшее из трех чисел. Тогда

$$lm > k^2 \geq k^2 - k + 1 = f(k) > 0.$$

Что противоречит тому, что $f(k)$ делится на lm.

Ответ. Не существует

4. См. рисунок. Заметим, что $\angle BMD = \angle EDM$, как накрест лежащие. Треугольник DKL равнобедренный. Значит $\angle KLD = \angle LKD$. Кроме того $\angle KLD = \angle LKB$, как накрест лежащие. Следовательно KL – биссектриса $\angle BKD$, а DM – биссектриса $\angle EDK$. Заметим, что эти углы – внешние углы треугольника



KCD, а *CA* – биссектриса третьего угла этого треугольника. Следовательно все биссектрисы пересекаются в одной точке *O*. (Замечание. В старших классах этот факт должен быть очевиден. Это прямое следствие из того, что биссектриса угла есть геометрическое место точек равноудаленных от сторон угла. Поэтому, если этот факт не доказывается, баллы не снимаются).

5. **Решение**: Поскольку НОД(a, 33) = 3, то при зашифровании три разные буквы переходят в одну. Так "А", "К" и "Х" переходя в "О"; буквы "Б", "Л", "Ц" – в "Ъ" и т.д. Поэтому, по полученному ширфтексту математически однозначно нельзя определить, какое сообщение было изначально. Поскольку известно, что изначально было осмысленное выражение, то восстановить его можно с помощью бесключевого чтения, т.е. перебором, подбирая буквы так, чтобы выстраивалась осмысленная последовательность русских слов.
   Ответ: ВСЕ ГОВОРИЛИ ЧТО Я НЕ РАЗБЕРУСЬ С АФФИННЫМ ШИФРОМ.
6. **Решение**: Заметим, что при любой таблице замены в шифре простой замены при повторном зашифровании любого символа рано или поздно происходит зацикливание, т.е. символ переходит сам в себя. Длина такого цикла может варьироваться от 1, когда символ при одинарном зашифровании переходит в себя, до m (где m – размер алфавита), например, при шифре сдвига с ключом 1. При этом легко убедиться, что любое промежуточное значение длины цикла достижимо. Значит, если в алфавите m символов, то гарантированно за НОК(1, 2, 3, ..., m) повторов операций зашифрования любой символ перейдет сам в себя. При этом, это минимальное число, обладающее таким свойством. Также заметим, что и за любое число зашифрований вида k * НОК(1, 2, 3, ..., m) любой символ гарантированно перейдет сам в себя.
   Раз за 24504479 зашифрований Y перешел в X, то это значит, что за 24504480 зашифрований X переходит в X.
   24504480 = 32*9*5*7*11*13*17. Перебирая все натуральные m начиная с 1, можно заметить, что пока $m < 19$, получающийся НОК будет делителем заданного числа. Но как только выберем $m \geq 19$, у искомого НОК-а появиться делитель 19, которого нет у заданного числа. Это, например, означает, что если мы возьмем шифр простой замены, в котором есть цикл длины 19, то за 24504480 зашифрований не все символы смогу перейти сами в себя.
   Ответ: От 1 до 18.