Олимпиада ФПМИ-2022 9-10 классы

Предварительные решения

1. Известно, что для чисел a, b и c выполняются равенства: $a^3 - b^3 - c^3 = 3abc$ и $a^2 = 2(b + c)$. Найдите число a.

Решение

Рассмотрим выражение $x^3 + y^3 + z^3 - 3xyz$ и разложим его на множители: $x^3 + y^3 + z^3 - 3xyz = (x + y)(x^2 - xy + y^2) + z^3 - 3xyz = (x + y)((x + y)^2 - 3xy) + z^3 - 3xyz = (x + y)^3 + z^3 - 3xy(x + y) - 3xyz = (x + y + z)((x + y)^2 - (x + y)z + z^2) - 3xy(x + y + z) = (x + y + z)(x^2 + y^2 + z^2 - xy - yz - zx)$.

Заметим также, что выражение во второй скобке может принимать только неотрицательные значения, то есть, $x^2 + y^2 + z^2 \geq xy + yz + zx$, причем равенство достигается тогда и только тогда, когда $x = y = z$.

Пусть $x = a$, $y = -b$, $z = -c$, тогда $a^3 - b^3 - c^3 - 3abc = (a - b - c)(a^2 + b^2 + c^2 + ab - bc + ca)$. По доказанному выше, равенство $a^3 - b^3 - c^3 = 3abc$ выполняется если a = b + c или a = –b = –c.

Из равенства $a^2 = 2(b + c)$ в первом случае получим, что $a^2 = 2a \Leftrightarrow a = 0$ или $a = 2$, а во втором случае: $a^2 = -4a \Leftrightarrow a = 0$ или $a = -4$.

Ответ; – 4, 0, 2,

2. Найдите все многочлены $P(x)$, для которых верно тождество

$$(x-1)P(x+1) \equiv (x+2)\left(P(x)-2022\right)$$

Решение

Подставим x=1. Получим $P(1)$=2022. Затем подставим x=0, получим $P(0)$=1011. Затем положим x=–1, получим P(–1)=0. Следовательно $P(x)=\left(x^3-x\right)Q(x)+ax^2+bx+c$. Подставляя в данное выражение –1, 0, 1, получим систему линейных уравнений для нахождения коэффициентов квадратного трехчлена. Получим

$P(x)=\left(x^3-x\right)Q(x)+1011(x+1)$ Подставим это выражение в исходное тождество

$$(x-1)x(x+1)(x+2)Q(x+1)+1011(x-1)(x+2) \equiv (x+2)x(x+1)(x-1)Q(x)+1011(x+2)(x-1).$$

Откуда получим, что при всех значениях переменных (за исключением четырех точек –2, –1, 0, 1) верно равенство $Q(x+1) \equiv Q(x)$, что означает, что $Q(x)=c$, где c – любое число. Соответственно $P(x)=c\left(x^3-x\right)+1011(x+1)=(x+1)\left(cx^2-cx+1011\right)$. Простой подстановкой можно убедиться, что любое c подходит.

3. Определим на множестве натуральных чисел функцию $f(n)$ равную количеству пар натуральных чисел $a<b$ так, что НОК$(a,b)=n$. Например, $f(4)=2$, $f(6)=4$.

   a) Найдите все двузначные n такие, что $f(n)=5$.

   b) Сколько существует трехзначных чисел, таких что $f(n)=12$?

Решение

Для начала сделаем несколько утверждений.

Утверждение 1: Если $n=p^k$, то $f(n)=k$.

Доказательство: Если $b<n$, то НОК $(a,b)=b<n$. Остается $b=n$. В этом случае a может быть любым делителем n меньшим n. Таких делителей k, значит и пар k.

Утверждение 2: Если $n=p^kq^m$, то $f(n)=(k+1)(m+1)-1+km$.

Доказательство: Если $b=n$, то a – любой делитель меньше n => таких делителей $(k+1)(m+1)-1$. Т.к. НОК $(a, b)=n$, то одной из этих чисел имеет вид p^kq^x, а второе q^mp^y, где x-целое число от 0 до $(m-1)$ включительно, y- целое число от 0 до $(k-1)$ включительно. Значит всего таких пар mk (в каждой паре большее число равно b, а меньшее a).

Утверждение 3: Пусть $D(n)$ – количество делителей числа n. Тогда $f(n)\geq D(n)-1$.

Доказательство: Если $b=n$, то a – любой делитель меньше n, значит количество пар не меньше чем $D(n)-1$.

a) По утверждению 3 у числа n не более 6 делителей, значит не более двух простых. Если $n=p^k$, то по утверждению 1 $k=5$ и единственное возможное двузначное это 32. Если $n=p^kq^m$, то $(k+1)(m+1)-1+km=5$ => $2km+k+m=5$. При $k\geq 2$, $2km+k+m\geq 5m+2$ =>$m<1$ – невозможно. А при $k=1$ имеем $3m=4$.

Ответ: Только 32.

b) Если n имеет один простой делитель, то по утверждению 1 $n=p^{12}$, но таких трехзначных чисел нет. Если n имеет два простых делителя, то по утверждению 2 $n=p^kq^m$ и $(k+1)(m+1)-1+km=12$ => $2km+k+m=12$. Переберем по k:

$k=1$ => $3m=11$ – нет корней

$k=2$ => $5m=10$ =>$m=2$. Далее корней не будет в силу симметрии равенства.

Значит $n=(pq)^2$. Т.к. n- трехзначное, то $10\leq pq\leq 31$. Возможные значения для pq: 10; 14; 15; 21; 22; 26.

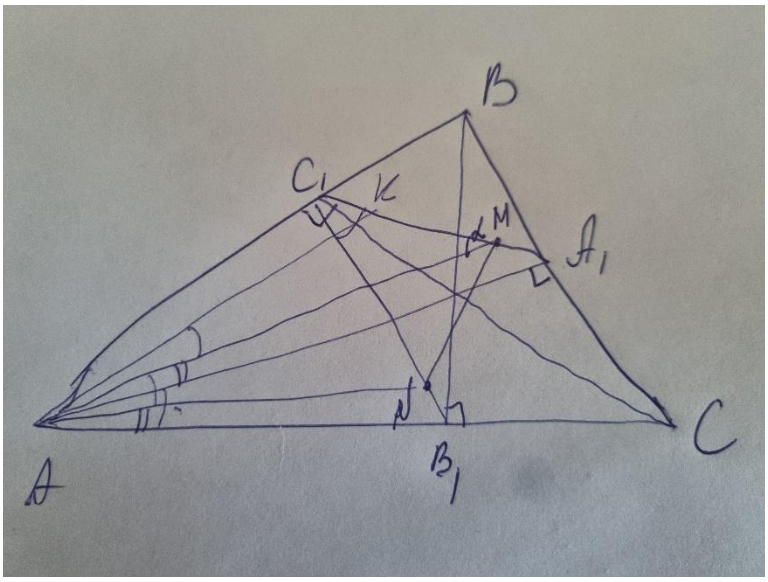
Если n имеет хотя бы 4 простых делителя, то D(n)≥16 и по утверждению 3 f(n)≥15.

Рассмотрим n=pqr, где p, q, r – простые числа. Тогда D(n)=8. Значит существует 7 пар при b=n. В любой паре хотя бы одной из чисел должно делиться на два простых множителя. Значит существуют пары: (pq; r); (pr; q); (qr; p); (pq; rq); (pq; rp); (rq; rp). Всего 6 пар. Значит в этом случае f(n)=13, что больше 12 и значит n не может иметь больше двух простых делителей.

Ответ: 6 чисел.

4. В остроугольном треугольнике ABC проведены высоты AA_1, BB_1, CC_1. На отрезках A_1C_1, C_1B_1 взяты соответственно точки M и N так, что $\angle MAA_1 = \angle NAC$. Найти $\angle AMN$, если $\angle AMC_1 = \alpha$.

Решение.



Заметим, что $\angle CCA_1 = \angle CBB_1$. Кроме того около четырехугольников ACA_1C_1 и BCB_1C_1 можно описать окружности диметрами которых соответственно являются стороны AC и BC. Следовательно, $\angle A_1C_1C = \angle CAA_1 = \angle CBB_1 = \angle CC_1B_1$. Из условия следует, что $\angle A_1C_1B_1 = 2\angle MAN$. Проведем прямую симметричную AN относительно прямой AA_1. Пусть она пересекает A_1C_1 в точке K. Т.к. $\angle KAN = \angle KC_1N$, то вокруг четырехугольника KC_1AN можно описать окружность. Заметим, что $\angle A_1C_1A + \angle B_1C_1A = 180^\circ$. Тогда $\angle KC_1A + \angle NC_1A = 180^\circ$. Откуда следует, что $\angle KC_1A = \angle KNA$. И тогда AK=AN. Т.е. $\triangle KAM = \triangle NAM$. AM – биссектриса угла C_1MN. Следовательно, $\angle AMN = \alpha$. Случай, когда K лежит на продолжении отрезка C_1A_1, рассматривается аналогично.

(9–10 класс) - КРИПТОГРАФИЯ

5. Знайка придумал новый шифр. Он записал 32 буквы русского алфавита (Е = Ё) в клетки таблицы 4 на 8. Чтобы зашифровать сообщение, его надо разбить на пары букв слева направо (пробелы и знаки препинания удаляются). Если количество букв в сообщении нечетное, то последняя буква повторяется дважды. Каждая пара букв зашифровывается по отдельности по следующим правилам: если буквы пары находятся в одной строке или одном столбце таблицы, то просто меняется порядок следования букв в паре; иначе, буквы пары соответствуют двум противоположным углам прямоугольника в таблице и при шифровании они заменяются на 2 буквы, соответствующие двум другим вершинам прямоугольника (при этом первой записывается та буква, которая находится в той же строке, что и первая буква исходной пары).

Знайка использовал представленную таблицу (при передаче часть букв в таблице потерялась). Например, слово "КРИПТОНН" будет зашифровано как "РКПИДЛНН". Незнайка получил от Знайки следующее сообщение:

Е	Х	Р	Д	Э	Т	Щ	С
?	Я	Г	П	?	?	?	И
?	Ш	Н	О	?	Л	Ю	?
?	?	К	Ц	?	?	?	?

ЧР ОД ЧЭ ХГ УВ ЯЦ ЛР ГЫ ЫЯ НК ПО ЧО ЬР

Помогите Незнайке расшифровать данное сообщение. (Исходное сообщение является осмысленной фразой на русском языке).

Ответ: "НЕ ДОВЕРЯЙ ШПУНТИКУ И КНОПОЧКЕ ".

Решение. Расшифрование осуществляется по тому же алгоритму, что и зашифрование. Рассмотрим первые 4 пары шифртекста "ЧР ОД ЧЭ ХГ" в зависимости от расположения буквы Ч возможны следующие 13 вариантов расшифрования: "ГЕ ДО ?Е РЯ", "НЕ ДО ?Е РЯ", "КЕ ДО ?Е РЯ", "КХ ДО ?Х РЯ", "ГЭ ДО ЭЧ РЯ", "НЭ ДО ЭЧ РЯ", "КЭ ДО ЭЧ РЯ", "ГТ ДО ?Т РЯ", "КТ ДО ?Т РЯ", "ГЩ ДО ?Щ РЯ", "КЩ ДО ?Щ РЯ", "НС ДО ?С РЯ", "КС ДО ?С РЯ". Поскольку это должно быть началом осмысленного текста на русском языке, то потенциально подходит второй варианты (с натяжкой еще подходит третий вариант). Значит предположительно мы нашли позицию буквы Ч (первый столбец, третья строка). Рассмотрим последние 4 пары в шифртексте, первые три пары расшифровываются однозначно, последней есть 12 вариантов: "КН ОП ОЧ (ГЕ, КЕ, КХ, ГЭ, НЭ, КЭ, ГТ, КТ, ГЩ, КЩ, НС, КС). Перебирая возможные концовки строк, получаем, что единственной подходящей является окончание "КЕ". Откуда находим позицию буквы "Ь". Вернемся к расшифровке первых 4 пар: "НЕ ДО ?Е РЯ". Вместо ? должна стоять одна из букв, которая еще не записана в таблице. В таблице еще не записаны буквы А, Б, В, Ж, З, Й, М, У, Ф, Ъ, Ы. Перебирая эти буквы, получаем, что подходят только буквы В и М. Нам уже известно следующее:

Е	Х	Р	Д	Э	Т	Щ	С
З	Я	Г	П	Б	Ъ	А	И
Ч	Ш	Н	О	В	Л	Ю	Ж
Ь	У	К	Ц	Й	М	Ф	Ы

Е	Х	Р	Д	Э	Т	Щ	С
?	Я	Г	П	?	?	?	И
Ч	Ш	Н	О	В или М	Л	Ю	?
Ь	?	К	Ц	?	?	?	?

Буква Ы не может стоять во второй строке или втором столбце, т.к. иначе последние 5 пар будут расшифровываться, как "ЯЫ КН ОП ОЧ КЕ". "ЯЫ" не могут быть в одном слове русского языка и нет слов, начинающихся на ЫКН...Небольшим перебором и рассмотрением расшифрования пар "ЛР ГЫ ЫЯ", можно показать, что единственное правдоподобное место буквы Ы это позиция в правом нижнем углу таблицы (четвертая строка, восьмой столбец).

Запишем, что нам уже удалось расшифровать:

"НЕ ДО (В,М)Е РЯ ?? П* НТ ИК *И КН ОП ОЧ КЕ" (Если знать персонажей Незнайки, то уже можно расшифровать сообщение). Звездочкой обозначена одна и та же буква в таблице. Перебирая оставшиеся варианты для *, получаем, что подходит только У. Далее простейшим перебором находим подходящий ответ.

Е	Х	Р	Д	Э	Т	Щ	С
?	Я	Г	П	?	?	?	И
Ч	Ш	Н	О	В или М	Л	Ю	?
Ь	*	К	Ц	?	?	?	?

6. В известном шифре RSA используется 2 ключа: e – открытый ключ для шифрования сообщений (зашифровывать сообщения может любой желающий) и d – закрытый ключ для расшифрования сообщений (расшифровывать может лишь тот, кто знает закрытый ключ). Ключи выбираются следующим образом: сначала выбираются 2 простых различных числа p и q, затем выбирается целое число e из промежутка от 1 до m ($m = (p-1)(q-1)$) так, что НОД(e, m) = 1, Наконец, число d выбирается как решение уравнения: $de \equiv 1 \pmod{m}$. Запись $a \equiv b \pmod{m}$ означает, что числа a и b дают одинаковые остатки при делении на m.

Игорь выбрал 2 простых числа p и q меньших 50. Перебрав все возможные значения для числа e и найдя соответствующие d, оказалось что ровно в 32 случаях числа e и d совпали. Найдите все возможные значения p и q, при которых такое могло произойти.

Ответ: (29, 31) и (41, 43).

Решение: По условию числа e и d связаны соотношением $de \equiv 1 \pmod{m}$. Если для некоторого e оказалось, что $d = e$, то такое e является решением уравнения $e^2 - 1 \equiv 0 \pmod{m}$. Оказывается, верно и обратное утверждение. Если e является решением уравнения $e^2 - 1 \equiv 0 \pmod{m}$, то НОД($e$, m) = 1 (это легко доказать от противного) из чего следует, что линейное уравнение $de \equiv 1 \pmod{m}$ имеет единственное решение относительно d, в качестве которого можно взять e. Таким образом, количество различных значений e, для которых d совпадает с e, равно количеству решений уравнения $e^2 - 1 \equiv 0 \pmod{m}$.

Найдем количество решений уравнения $e^2 - 1 \equiv 0 \pmod{m}$. Пусть $m = p_1^{\alpha_1} \cdot \ldots \cdot p_d^{\alpha_d}$. Если уравнение $e^2 - 1 \equiv 0 \pmod{p_i^{\alpha_i}}$ имеет T_i решений, то по китайской теореме об остатках можно показать, что исходное уравнение будет иметь $T_1 \cdot T_2 \cdot \ldots \cdot T_d$ решений. Значит, необходимо рассмотреть уравнение $e^2 - 1 \equiv 0 \pmod{p^\alpha}$ при различных значениях p.

Пусть $p > 2$, тогда исходное уравнение равносильно $(e-1)(e+1)$ делится на p^α. Заметим, что числа $(e-1)$ и $(e+1)$ одновременно на p делится не могут, откуда получаем только 2 возможных случая: либо $e - 1$ делится на p^α, откуда $e = 1$, либо $e + 1$ делится на p^α, откуда $e = p^{\alpha} - 1$. Таким образом, при $p > 2$ уравнение $e^2 - 1 \equiv 0 \pmod{p^{\alpha}}$ всегда имеет ровно 2 решения.

Пусть $p = 2$. Если $\alpha = 1$, то уравнение $e^2 - 1 \equiv 0 \pmod 2$ имеет единственное решение $e = 1$. Если $\alpha = 2$, то уравнение $e^2 - 1 \equiv 0 \pmod 4$ имеет 2 решения $e = 1$ и $e = 3$. Если $\alpha = 3$, то уравнение $e^2 - 1 \equiv 0 \pmod 8$ имеет 4 решения $e = 1$, $e = 3$, $e = 5$, $e = 7$. Пусть $\alpha > 3$, покажем, что и в этом случае уравнение будет иметь ровно 4 решения. Имеем $(e - 1)(e + 1)$ делится на 2^{α}. Заметим, что если одно из чисел $(e - 1)$ или $(e + 1)$ делится на 2^k ($k>1$), то второе из этих чисел делится только на 2. Действительно, пусть $e - 1 = 2^k l$, где l – нечетное число, тогда $e + 1 = e - 1 + 2 = 2^k l + 2 = 2\,(2^{k-1} l + 1)$, где $2^{k-1} l + 1$ – нечетное. Таким образом, получаем 4 возможных варианта: 1) $(e - 1)$ делится на 2^{α}, откуда $e = 1$; 2) $(e - 1)$ делится на $2^{\alpha-1}$, откуда $e = 2^{\alpha-1} + 1$; 3) $(e + 1)$ делится на $2^{\alpha-1}$, откуда $e = 2^{\alpha-1} - 1$; 4) $(e + 1)$ делится на 2^{α}, откуда $e = 2^{\alpha} - 1$. Итак, уравнение $e^2 - 1 \equiv 0 \pmod{2^{\alpha}}$ имеет 1 решение при $\alpha = 1$, имеет 2 решения при $\alpha = 2$ и имеет 4 решения при $\alpha \geq 3$.

Представим m в следующем виде: $m = 2^{\alpha} \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_d^{\alpha_d}$, где $p_1, \ldots, p_d$ – нечетные простые числа. Уравнение $e^2 - 1 \equiv 0 \pmod m$ будет иметь ровно 32 корня в одной из следующих четырех ситуаций: 1) $\alpha = 0$, $d = 5$; 2) $\alpha = 1$, $d = 5$; 3) $\alpha = 2$, $d = 4$; 4) $\alpha \geq 3$, $d = 3$. Посмотрим, какие делители содержат простые числа, меньшие 50 и какие из описанных выше 4 ситуаций возможны, когда $m = (p - 1)(q - 1)$.

p	2	3	5	7	11	13	17	19
$p - 1$	1	2	$4=2^2$	$6=2\cdot 3$	$10=2\cdot 5$	$12=2^2\cdot 3$	$16=2^4$	$18=2\cdot 3^2$

p	23	29	31	37	41	43	47
$p - 1$	$22 = 2\cdot 11$	$28=2^2\cdot 7$	$30=2\cdot 3\cdot 5$	$36=2^2\cdot 3^2$	$40=2^3\cdot 5$	$42 = 2\cdot 3\cdot 7$	$46=2\cdot 23$

Перебирая все варианты видим, что только 2 пары чисел подходят: (29, 31) и (41, 43).