Пример нахождения подхода к решению задачи всеросса по аналогии с теорией квадратичных вычетов.

Никишин Максим, 57 школа, 2021 год.

Изучая в математической литературе различные способы решения задач, мы часто ловим себя на том, что, понимая авторское решение, не понимаем, каким образом к нему пришел сам автор. В то же время во многих случаях понимание пути, на котором можно найти решение, имеет гораздо большую ценность чем сам результат.

В данной работе показано, как поиск аналогий с задачами, успешно решаемыми с помощью формализма квадратичных вычетов, помог найти решение задачи даже не смотря на то, что сама теория квадратичных вычетов при ее решении так и не понадобилась.

Пусть натуральные числа $n > 20$ и $k > 1$ таковы, что n делится на k^2. Докажите, что найдутся натуральные числа a, b, c такие что $n = ab + bc + ca$.

Идея : очевидное представление $n = ab + bc + ac = c\,(a + b) + ab$ наводит на мысль о том, что критерий представимости это принадлежность n классу вычетов дающего остаток ab по модулю $(a + b)$ это хорошо тем что $ab \equiv -a^2 \pmod{a + b}$. Тогда можно положить $a + b = q$, где q простое число, чтобы можно было работать с квадратичными вычетами и задача сводится к нахождению q.

Пусть p–наибольший простой делитель k, тогда $n = a\,k^2 = a\,(p\,y)^2 = p^2\,x$, где $x = a\,y^2$.

Итак $n = p^2\,x$

Рассмотрим два случая : $x \geq p$ и $x < p$

1. Если $x \geq p$, можно заметить, что при $a = p$, $b = p^2 - p$ и $c = x + 1 - p$

$ab + bc + ca = p\,(p^2 - p) + (p^2 - p)\,(x + 1 - p) + (x + 1 - p)\,p = x\,p^2 = n$

А это и требовалось доказать.

Заметим, что если простое $p < 5$ (то есть p не больше трех), то из условия, что $n > 20$ следует

$9\,x > p^2\,x = n > 20, \Rightarrow x \geq 3 \geq p$ (т.к. $3^2 * 2 = 18 < 20$) $\Rightarrow x \geq p$,

что становится дополнительным условием на p в случае 2 :

2. Если $x < p > 5$.

То есть, нужно доказать что числа :

$p^2,\ 2\,p^2,\ 3\,p^2,\ \ldots,\ (p - 1)\,p^2$

представимы в виде $ab + bc + ca$.

Любое нечетное число представимо как

$m\,1 + m\,1 + 1 \times 1 = 2\,m + 1$, где $m \in \mathbb{N}$ (то есть $a = 1;\ b = m;\ c = 1;$)

Любое число кратное 4 представимо как

$m\,2 + m\,2 + 2 \times 2 = 4\,(m + 1)$

где $m \in \mathbb{N}$ (то есть $a = 2;\ b = m;\ c = 2;$)

Но тогда остаются лишь $n = p^2 x$, где $0 < x < p$ и $x = 4k + 2$, где $k \in \mathbb{N}$.

Пусть для некоторого простого q :

$(n > q^2) \bigwedge (n + a^2 \vdots q \Rightarrow n = q\,t - a^2,\ t \in \mathbb{N}) \bigwedge (0 < a < q)$

Сделаем в выражении $n = q\,t - a^2$ замену $t = c + a$, что возможно в силу произвольности выбора c

$n = q\,t - a^2 = q\ (c + a) - a^2 = qc + a\ (q - a) = (a + q - a)\ c + a\ (q - a) = ac + (q - a)\ c + a\ (q - a)$

и $a\ (q - a) < q^2 \Rightarrow c > 0 \Rightarrow$

такие n представимы (с точностью до замены $q - a = b$) в виде $ab + bc + ca$.

Из условий на q следует, что n (а следовательно и x)

является квадратичным вычетом по модулю q, если $q = 4d + 1$.

Или квадратичным невычетом, если $q = 4d + 3$ (по свойствам квадратичных вычетов,

а именно, -1 является квадратичным вычетом по модулю q, если $q = 4d + 1$.

Или квадратичным невычетом, если $q = 4d + 3$).

Эти соображения помогают найти q.

Докажем, что для всех

$n = p^2 x = p^2\ (4k + 2)$

найдётся такое простое число q

(напоминаем, что случай с $x = 4k + 2$ единственный оставшийся недоказанным).

Добавим единицу с обеих сторон равенста $x = 4k + 2$ и получим $x + 1 = 4k + 3$,

$4k + 3$ имеет простой делитель q вида $4d + 3 = q$ $(d \in \mathbb{N})$

поскольку остаток произведения равен произведению остатков.

$x + 1 \vdots q \Leftrightarrow x \equiv -1 \pmod q$ тогда так как

$p^2\ (x + 1) \vdots q$

$n = p^2 x \equiv -p^2 \equiv -a^2 \pmod q$ где a есть остаток $p \pmod q$ то есть $n + a^2 \vdots q$

при этом $(p \geq x + 1 \geq q) \wedge (x > 1) \Rightarrow$

$n = p^2 x > p^2 \geq q^2 \Rightarrow \mathbb{N} > q^2$.

Значит такое q подходит и все числа $p^2 x$ $0 < x < p$ представимы в виде $ab + bc + ca$.