Натуральные и целые числа знакомы вам с младших классов, но полезно и поучительно подойти к ним, владея аппаратом алгебры. Задачи о делимости и уравнения в целых числах служат излюбленным материалом для математических олимпиад и факультативов. Некоторые разбираемые примеры и задачи для самостоятельного решения предлагались на Российской математической олимпиаде, вступительных экзаменах в МФТИ, МГУ и другие вузы. В последнее время задачи с целыми числами регулярно встречаются в частях С заданий единого госэкзамена. Рекомендованные пособия помогут вам в решении задач и более глубоком проникновении в эту тему.

## § 1. Делимость целых чисел. Простые и составные числа. Основная теорема арифметики

Напомним некоторые понятия и факты.

Числа 1, 2, 3 и так далее, используемые для счёта, называются *натуральными.* Наименьшее натуральное число – это 1, а наибольшего натурального числа не существует. Целые числа – это числа …–3, –2, –1, 0, 1, 2, 3,…; ряд целых чисел можно неограниченно продолжить как вправо, так и влево.

Натуральное число $n$ называется *делителем* целого числа $m$, если $m = nk$ для подходящего целого числа $k$. В этом случае говорят, что $m$ *делится* на $n$ (нацело) и обозначают этот факт так: $m \vdots n$ (иногда используют обозначение $n \mid m$, что означает «$n$ делит $m$»). Число $m$ также называют *кратным* числу $n$. Каждое число $n$ имеет бесконечное множество кратных: $0, \pm n, \pm 2n, \pm 3n, \ldots$

Натуральное число, имеющее ровно два различных делителя – само себя и единицу, – называется *простым*. Целое число, имеющее больше двух различных делителей, называется *составным.* Наименьшее простое число равно 2. Остальные простые числа являются нечётными. Согласно определению, число 1 – ни простое, ни составное.

Если целые числа $m$, $n$ делятся на натуральное число $c$, то $c$ называется их *общим делителем*. *Наибольший общий делитель* $m$ и $n$ обозначается НОД($m$, $n$) (иногда также ($m$, $n$)). Он делится на любой общий делитель данных чисел.

Любое целое число, кратное $m$ и $n$, называется их *общим кратным.* Наименьшее натуральное число, кратное $m$ и $n$, называется *наименьшим общим кратным* $m$ и $n$. Оно обозначается НОК($m$, $n$) (иногда также [$m$, $n$]). Наименьшее общее кратное чисел $m$ и $n$ делит любое общее кратное этих чисел.

Целые числа, не имеющие общих делителей, кроме 1, называются *взаимно простыми.*

Вам известны формулы сокращённого умножения:

$$a^2 - b^2 = (a-b)(a+b);\ \ a^3 + b^3 = (a+b)(a^2 - ab + b^2);$$

 

$$a^3 - b^3 = (a-b)(a^2 + ab + b^2).$$

Их обобщением являются две следующие формулы ($n$ – натуральное число):

(I) $$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1});$$

(II) $$a^{2n+1} + b^{2n+1} = (a+b)(a^{2n} - a^{2n-1}b + \cdots + ab^{2n-1} + b^{2n}).$$

Из этих тождеств видно, что при целых *a, b* разность любых натуральных степеней и сумма нечётных степеней $a$ и $b$ делятся соответственно на $a - b$ и $a + b$.

В этом задании нам понадобится

**Метод математической индукции** для доказательства утверждений, зависящих от $n$**.** Согласно этому методу, ***если***

**(1)** ***доказываемое утверждение верно для начального значения*** $n = n_0$ **(чаще всего** $n_0 = 1$**, но иногда и 0) ("основание индукции"),** ***и если***

**(2)** ***из предположения, что доказываемое верно для некоторого*** $n = k$ **("предположение индукции")** ***следует его справедливость для*** $n = k + 1$ **("шаг индукции"),** ***то утверждение верно для всех целых*** $n \geq n_0$**.**

Следует подчеркнуть, что нельзя пренебрегать ни основанием, ни шагом индукции.

Сформулируем **основные свойства делимости.**

**Свойство 1.** Если целое число $a$ делится на $m$, а $m$ делится на $k$, то $k$ является делителем $a$.

**Свойство 2.** Пусть $a$ и $b$ – целые числа, $n$ – их общий делитель. Тогда: 1) $a + b$ , $a - b$ делятся на $n$; 2) $ab$ делится на $n^2$.

**Следствие** (из свойства 2). Если одно из чисел $a$ или $b$ делится на $n$, а второе не делится, то $a + b$ , $a - b$ не делятся на $n$.

В самом деле, если допустить, что $a$ и $a + b$ делятся на $n$, то и $b = (a + b) - a$ делится на $n$, согласно свойству 2(1), вопреки условию.

**Свойство 3.** Если целое число $a$ делится на взаимно простые натуральные числа $m$ и $n$, то $a$ делится на их произведение $mn$. В общем случае $a$ делится на НОК($m$, $n$) (которое равно $mn$, если $m$, $n$ взаимно просты).

**Свойство 4.** Если $a$, $b$ – целые числа, $p$ – простое число и $ab$ делится на $p$, то $a$ или $b$ делится на $p$.

**Свойство 5.** Если $a$, $b$ – целые числа, $ab$ делится на натуральное число $n$, причём $b$ и $n$ взаимно просты, то $a$ делится на $n$.

На основе этих свойств можно устанавливать, что некоторые числовые выражения представляют собой составные числа.

**Пример 1.** Проверить, что данные числа являются составными:

а) $3148^3 - 1139^3$; б) $39^9 + 512$; в) $7 \cdot 13 \cdot 19 \cdot \ldots \cdot 67 - 2010$.

 

***Решение.*** а) по формуле разности кубов, $3148^3 - 1139^3 = (3148 - 1139)\cdot(3148^2 + 3149\cdot1139 + 1138^2)$ делится на $3148 - 1139 = 2009$;

б) в силу формулы (II) для суммы нечётных степеней, $39^9 + 512 = 39^9 + 2^9$ делится на $39 + 2 = 41$ (впрочем, можно было бы обойтись суммой кубов: $39^9 + 2^9 = (39^3)^3 + (2^3)^3$);

в) поскольку $2010 = 30\cdot67$ (проверьте), то $7\cdot13\cdot19\cdot\ldots\cdot67 - 2010$ делится на 67.

Задачи проверки простоты и разложения на два множителя больших составных чисел весьма трудоёмки даже для современных компьютеров. Уже поиск первого простого делителя может оказаться сложным. На практике можно использовать следующие утверждения.

***Наименьший (больший 1) делитель k составного числа n является простым:*** если $n = kl$, причём $k = pq$, где $1 < p < k$, *то* $p$ – делитель числа $n$, меньший $k$.

***Если число n составное: n = ab, то квадрат одного из сомножителей не превосходит n, то хотя бы один из сомножителей не превосходит*** $\sqrt{n}$. Действительно, допустив противное, что $a > \sqrt{n}, b > \sqrt{n}$, и перемножив два этих неравенства, мы получили бы, что $ab > \sqrt{n}\cdot\sqrt{n} = n$ – противоречие.

Разберём метод разложения натурального числа на множители, не требующий перебора всевозможных его простых делителей. Этот оригинальный метод был предложен знаменитым французским математиком Пьером Ферма (1601–1665).

Предварительно выведем легко запоминающуюся формулу для суммирования последовательных нечётных чисел. Заметим, что $1=1^2$, $1+3=2^2$, $1+3+5=3^2$, $1+3+5+7=4^2$. Появляется предположение, что $S_n = 1 + 3 + \ldots + (2n-1) = n^2$ для любого натурального $n$.

Учтём, что $S_n = 1+3+\ldots+(2n-1)$ – это сумма $n$ последовательных членов арифметической прогрессии с первым членом 1 и последним $2n - 1$:

$$1 + 3 + \ldots + (2n-1) = \frac{(1 + (2n-1))n}{2} = n^2,$$

что и требовалось доказать.

Теперь изложим ***метод Ферма***. Пусть $n > 3$ – нечётное натуральное число. Будем прибавлять к нему последовательно нечётные числа 1, 3, 5, 7 и т. д., пока не получим квадрат некоторого числа $l$: $n + 1+3+5+7 +\ldots +(2k-1) = l^2$. Так как $1+3+5+\ldots+(2k-1) = k^2$, то $n = l^2 - k^2 = (l - k)(l + k)$ – искомое разложение числа $n$.

 

**Пример 2.** Разложить на множители число 2009.

*Решение*. Само число 2009 не является квадратом ($44^2 = 1936$, $45^2 = 2025$). Будем прибавлять к числу 2009 последовательные нечётные числа до получения квадрата: $2009+1+3+5+7 = 2025 = 45^2$, то есть $2009 + 4^2 = 45^2$. Тем самым $2009 = 45^2 – 4^2 = (45 – 4)(45 + 4) = 41\cdot49 = 41\cdot7^2$.

**Ответ:** $2009 = 41\cdot7^2$.

Разберём примеры, в которых требуется разложить на множители число, заданное алгебраическим или числовым выражением, либо выяснить его простоту.

**Пример 3**. При каких целых значениях $n$ число $3n^4 - 10n^2 + 3$ является простым? Найти это простое число.

***Решение.*** Чтобы разложить данное выражение на множители, можно ввести $t = n^2$ и найти корни уравнения $3t^2 - 10t + 3 = 0$: $t_1 = 3, t_2 = \frac{1}{3}$, следовательно, $3n^4 - 10n^2 + 3 = 3(n^2 - 3)(n^2 - \frac{1}{3}) = (n^2 - 3)(3n^2 - 1)$. Для того, чтобы это выражение имело простое значение, необходимо, чтобы одна скобка равнялась 1, в то время как вторая была простым числом.

Если $n^2 - 3 = 1$, то $n = \pm 2$, при этом $3n^2 - 1 = 11$ – простое число. Второй случай $3n^2 - 1 = 1$, $3n^2 = 2$ невозможен при целом значении $n$.

**Ответ:** при $n = \pm 2$ число равно 11.

В следующем примере применяется метод выделения полного квадрата. Выделение квадрата возможно в двух ситуациях:

1) когда есть квадрат первого числа и удвоенное произведение первого на второе, надо добавить и вычесть квадрат второго числа;

2)когда есть сумма квадратов двух чисел, надо добавить и вычесть их удвоенное произведение.

**Пример 4.** Может ли число $n^4 + 64$ быть простым при каких-либо целых $n$?

***Решение.*** Дополним выражение $n^4 + 64 = (n^2)^2 + 8^2$ до квадрата суммы:

$(n^2)^2 + 2n^2\cdot8 + 8^2 – 16n^2 = (n^2 + 8)^2 – (4n)^2 = (n^2 – 4n + 8)(n^2 + 4n + 8) = ((n – 2)^2 + 4)((n + 2)^2 + 4)$. Ясно, что обе скобки не меньше 4, так что данное выражение всегда представляет собой составное число.

**Ответ:** число $n^4 + 64$ составное при любом целом значении $n$.

**Пример 5.** Разложить $2^{32} + 2^{16} + 1$ на два множителя, большие 30 000.

***Решение.*** Воспользуемся выделением полного квадрата:

$2^{32} + 2^{16} + 1 = (2^{16})^2 + 2\cdot 2^{16} + 1 - 2^{16} = (2^{16} + 1)^2 - (2^8)^2 = (2^{16} + 1 - 2^8)(2^{16} + 1 + 2^8)$ по формуле разности квадратов. Оценим сомножители:
$2^{16} + 1 - 2^8 > 2^8(2^8 - 1) > 2^8 \cdot 2^7 = 2^5 \cdot 2^{10} > 32 \cdot 1000 = 32 \cdot 1000$,
вторая скобка еще больше.

Рассмотрим применение тождеств (I) и (II).

**Пример 6.** Доказать, что число $z = 15^n - 8^n + 6\cdot 36^n + 1$ делится на 14 при любом натуральном значении числа $n$.

***Решение.*** По формуле (I):

$15^n - 8^n = (15 - 8)(15^{n-1} + \cdots + 15 \cdot 8^{n-2} + 8^{n-1})$ делится на 7.

Третье слагаемое запишем как степень шести: $6\cdot 36^n = 6^{2n+1}$. Применим к третьему и четвёртому слагаемым формулу (II):

$$6^{2n+1} + 1 = (6 + 1)(6^{2n} - 6^{2n-1} + \cdots - 6 + 1).$$

Так как $z = (15^n - 8^n) + (6 \cdot 36^n + 1)$ и обе скобки делятся на 7, то $z$ делится на 7. Кроме того, числа $15^n+1$, $8^n$ и $6\cdot 36^n$ чётные, поэтому $z$ делится на 2. А так как числа 2 и 7 взаимно простые, то $z$ делится на $2\cdot 7 = 14$, согласно свойству 3.

При помощи свойств 4 и 5 можно доказать, что квадратный корень из простого числа $p$ есть число иррациональное, т.е. не представимое в виде обыкновенной дроби.

**Пример 7.** Доказать, что если $p$ – простое число, то число $a = \sqrt{p}$ иррациональное.

***Решение.*** Допустим противное, что $a$ является рациональным числом: $a = \frac{m}{n}$ для некоторых натуральных $m$ и $n$, причём дробь несократима, то есть $m$ и $n$ взаимно просты. Тогда $a^2 = \frac{m^2}{n^2} = p$, $m^2 = pn^2$, то есть $m^2$ делится на $p$. По свойству 4, $m$ делится на $p$, так что $m = pt$, $t$ натуральное, откуда $m^2 = p^2t^2 = pn^2 \Rightarrow n^2 = pt^2$. Из последнего равенства следует, что $n \vdots p$, то есть $m$, $n$ имеют общий делитель $p$, вопреки несократимости дроби $\frac{m}{n}$. Полученное противоречие доказывает, что допущение о рациональности $a$ неверно.

В заключение параграфа продемонстрируем, как доказывать делимость методом математической индукции.

 

**Пример 8.** Доказать, что при любом неотрицательном целом $n$ число $a_n = 5 \cdot 7^{2n+2} + 2^{3n}$ делится на 41.

***Доказательство.*** *Основание индукции*. При $n = 0$ число $a_0 = 5 \cdot 7^2 + 2^1 = 246 = 41 \cdot 6$ делится на 41.

Шаг индукции. Допустим, что для некоторого целого $k \geq 0$ число $a_k = 5 \cdot 7^{2k+2} + 2^{3k}$ делится на 41. Запишем $a_{k+1} = 5 \cdot 7^{2(k+1)+2} + 2^{3(k+1)} = 5 \cdot 7^{2k+4} + 8 \cdot 2^{3k}$ и вычислим разность

$$a_{k+1} - 8a_k = 5 \cdot 7^{2k+4} - 8 \cdot 5 \cdot 7^{2k+2} = 5 \cdot 7^{2k+2} \cdot (7^2 - 8) = 5 \cdot 7^{2k+2} \cdot 41.$$

Поскольку $a_k \vdots 41$, то $a_{k+1} = (a_{k+1} - 8a_k) + 8a_k \vdots 41$.

Таким образом, согласно принципу математической индукции, $a_n \vdots 41$ при всех $n = 0, 1, 2, \ldots$

 