Федеральное агентство по образованию
Федеральная заочная физико-техническая школа
при Московском физико – техническом институте
(государственном университете)

МАТЕМАТИКА

Элементы теории чисел

Задание №6 для 9-х классов

(2009-2010 учебный год)

г. Долгопрудный, 2010

Составитель: И.А. Чубаров, доцент кафедры высшей математики МФТИ.

Математика: задание №6 для 9-х классов (2009-2010 учебный год). - М.: МФТИ, 2009, 28с.

Дата отправления заданий по физике и математике – 23 апреля 2010 г.

Учащийся должен стараться выполнять **все** задачи и контрольные вопросы в заданиях. Некоторая часть теоретического материала, а также часть задач и контрольных вопросов являются сложными и потребуют от учащегося больше усилий при изучении и решении. В целях повышения эффективности работы с материалами они обозначены символом «*» (звездочка). Мы рекомендуем приступать к этим задачам и контрольным вопросам в последнюю очередь, разобравшись вначале с более простыми.

Составитель:
Чубаров Игорь Андреевич
Подписано 09.03.10. Формат 60x90 1/16.
Бумага типографская. Печать офсетная. Усл. печ. л. 1,5
Уч.-изд. л. 1,33. Тираж 1400. Заказ №17-з.

Федеральная заочная физико-техническая школа
при Московском физико-техническом институте
(государственном университете)
ООО «Печатный салон ШАНС»

141700, Москов. обл., г. Долгопрудный, Институтский пер., 9
ЗФТШ при МФТИ, тел/факс (495) 408-5145 – **заочное отделение**
тел./факс (498) 744-6351 – **очно-заочное отделение**
тел. (498) 744-6583 – **очное отделение**

e-.mail: ***zftsh@mail.mipt.ru***

Наш сайт: www.school.mipt.ru

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) $7\cdot13\cdot19\cdot\ldots\cdot67-2010$.

Решение. а) по формуле разности кубов, $3148^3 - 1139^3 = (3148 - 1139)\cdot(3148^2 + 3149\cdot 1139 + 1138^2)$ 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 $2010 = 30\cdot 67$ (проверьте), то $7\cdot 13\cdot 19\cdot\ldots\cdot 67 - 2010$ 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 $2009 = 45^2 - 4^2 = (45 - 4)(45 + 4) = 41\cdot 49 = 41\cdot 7^2$.

Ответ: $2009 = 41\cdot 7^2$.

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:

$(n^2)^2 + 2n^2\cdot 8 + 8^2 - 16n^2 = (n^2 + 8)^2 - (4n)^2 = (n^2 - 4n + 8)(n^2 + 4n + 8) =$ $= ((n - 2)^2 + 4)((n + 2)^2 + 4)$. 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: $a = \dfrac{m}{n}$ для некоторых натуральных m и n, причём дробь несократима, то есть m и n взаимно просты. Тогда $a^2 = \dfrac{m^2}{n^2} = p$, $m^2 = pn^2$, 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 $\dfrac{m}{n}$. 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

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

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 $n = 0, 1, 2, \ldots$

§2. Деление целых чисел с остатком. Основная теорема арифметики

Любое целое число а можно разделить с остатком на любое натуральное число n, т.е. представить а в виде

$$\boldsymbol{a = nq + r,\ 0 \leq r < n,} \qquad \text{(III)}$$

где q – целое число – *частное*, а r – *остаток* от деления a на n. *Частное q и остаток r определены однозначно.*

В самом деле, если допустить, что возможны два выражения $a = nq + r = sn + t,\ 0 \leq r \leq t < n,$ то $0 \leq t - r = n(q - s) < n,$ следовательно, $q = s \Rightarrow t = r$ – единственность доказана.

Например, при делении 2010 на 7 получим 2010 = 287 ·7 + 1. Для числа –2010 неверно было бы написать, что –2010 = –287·7 – 1, так как остаток должен быть положительным. Чтобы удовлетворить этому условию, вычтем из правой части 7 и прибавим к ней 7: –2010 = –287·7– 7+7–1 = –288·7 + 6, т.е. остаток равен 6. В общем случае при $a < 0$ надо вначале получить равенство $-a = sn + t, 0 < t < n,$ а затем провести такие преобразования:

$$a = -sn - t = -(s+1)n + (n - t), q = -s - 1, r = n - t\,.$$

Из теоремы о делении с остатком вытекает, что ***среди любых выписанных подряд n целых чисел ровно одно кратно n,*** а остальные дают при делении все остатки от 1 до n – 1 (причём эти остатки идут подряд, начинаясь, возможно, не с 1).

Поэтому ***чётные и нечётные числа чередуются, так что произведение*** $n(n+1)$ ***любых двух последовательных целых чисел делится на 2.***

Это утверждение часто применяется при решении задач.

Пример 9. Доказать, что при любом целом *n* число $9n^2+9n+2$ делится на 2.

Решение. Данное выражение разлагается на множители: $9n^2+9n+2=$ $=(3n+1)(3n+2)$, которые представляют собой два последовательных целых числа. Можно то же самое доказать проще, если учесть, что $9n^2+9n+2$ и $9n(n+1)$ имеют одинаковую чётность.

Далее, ***произведение*** $(n-1)n(n+1)$ ***любых трёх последовательных целых чисел делится на 3*** (по скольку все целые числа можно представить в виде $3k;\, 3k+1;\, 3k+2;\, k=0,\pm1,\pm2,\ldots$).

Кроме того, среди 3-х множителей встречаются два последовательных целых числа, а именно, $k-1$ и k или k и $k+1$. Отсюда следует, что ***при любом целом*** k ***произведение*** 3-х последовательных чисел ***делится на 6*** (по свойству 3, так как оно делится на взаимно простые числа 2 и 3).

Пример 10. Доказать, что для любого целого *n* число $a=\frac{n}{3}+\frac{n^2}{2}+\frac{n^3}{6}$ целое.

Решение. Сложим данные дроби: $a=\frac{n^3+3n^2+2n}{6}$. Разложим числитель на множители: $n^3+3n^2+2n=n(n^2+3n+2)=n((n^2+n)+(2n+2))=$ $=n(n(n+1)+2(n+1))=n(n+1)(n+2)$. Оказывается, числитель равен произведению трёх последовательных целых чисел и, как замечено, делится на 6, следовательно, данное число целое.

———— . ———— . ————

Произведение четырёх последовательных целых чисел $(n-1)n(n+1)(n+2)$ ***делится на*** **24**. Как показано выше, оно делится на 3. Кроме того, среди записанных четырёх сомножителей один делится на 4 и ещё один (через один от него) делится ровно на 2. Таким образом, по свойствам делимости, произведение делится на 8, а т.к. числа 3 и 8 взаимно простые, то оно делится на $3\cdot8=24$.

Пример 11. Доказать, что если натуральное число p взаимно просто с 6 и $p > 4$, то $p^2 - 1$ делится на 24.

Решение. Выражение $p^2 - 1 = (p-1)(p+1)$ – часть произведения $(p-1)\,p\,(p+1)(p+2)$, делящегося на $24 = 8{\cdot}3$. Так как p не делится на 2, то и $p + 2$ не делится на 2, так что $p(p+2)$ не делится на 2, поэтому $(p-1)(p+1)$ делится на 8. Кроме того, $(p-1)p(p+1) \vdots 3$, а p взаимно просто с 3, следовательно, $(p-1)(p+1)$ делится и на 3, а так как 8 и 3 взаимно просты, то $(p-1)(p+1)$ делится на 24, что и требовалось доказать.

Пример 12. Найти все простые числа p такие, что $p + 10$, $p + 14$ являются простыми.

Решение. Очевидно, $p > 2$, так как при $p = 2$, $p + 10 = 12$ и $p + 14 = 16$. Заметим, что числа p, $p + 10 = p + 1 + 9$, $p + 14 = p + 2 + 12$ дают разные остатки при делении на 3, поскольку p, $p + 1$, $p + 2$ – три последовательных натуральных числа. Следовательно, одно из этих чисел делится на 3. Если p делится на 3, то p равно трём. Если p не делится на 3, то $p + 10$ или $p + 14$ делятся на 3 и не могут быть простыми.

Ответ: $p = 3$.

Сформулируем ключевое для решения задач о делимости утверждение, известное как

<u>Основная теорема арифметики натуральных чисел.</u> ***Любое натуральное число n, большее единицы, можно разложить в произведение простых чисел. Это разложение единственно, с точностью до порядка следования сомножителей.***

Строгое доказательство этой теоремы первым дал К.Ф. Гаусс (1777 – 1855), немецкий математик, внёсший крупный вклад в алгебру, теорию чисел, математический анализ и другие разделы теоретической и прикладной математики. Это доказательство можно прочитать, например, в учебнике [3]. Если в разложении на множители числа n встречаются равные простые числа, их удобно собирать в степени. В результате получается

каноническое разложение: $$n = p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m} \qquad \textbf{(IV)},$$

где $p_1, \ldots, p_m$ – *различные простые числа.* Такое разложение абсолютно однозначно, если потребовать, чтобы $p_1 < \ldots < p_m$.

Например, $3780 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 7 = 2^2 \cdot 3^3 \cdot 5 \cdot 7$.

Следующий пример вполне можно решить с помощью простейшего калькулятора. Но наша цель – усвоить идеи и методы, чего можно достичь только при ручных вычислениях.

Пример 13. Найти все делители числа 496 и сумму его собственных делителей.

Решение. Разложим 496 на простые множители: $496 = 8{\cdot}62 = 2^4{\cdot}31$. Все делители: 1, 2, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$ и 31, $2{\cdot}31 = 62$, $4{\cdot}31 = 124$, $8{\cdot}31 = 248$ и само число 496. Сложим собственные делители, т.е. найденные числа, меньшие 496: $1 + 2 + 4 + 8 + 16 + 31 + 2{\cdot}31 + 4{\cdot}31 + 8{\cdot}31 =$ (для удобства подсчёта сгруппируем слагаемые) $= (1 + 31) + (2 + 2{\cdot}31) + (4 + 4{\cdot}31) + (8 + 8{\cdot}31) = 32{\cdot}(1 + 2 + 4 + 8) + 16 = 16{\cdot}(1 + 2 + 4 + 8 + 16) = 16{\cdot}31 = \underline{496}$.

Натуральное число, которое равно сумме его собственных делителей, принято называть <u>совершенным</u>.

При решении уравнений в целых числах приходится использовать разложение целых чисел не только на положительные, но и на отрицательные множители. В таком случае каноническим разложением следует считать разложение $n = (\pm p_1^{k_1})(\pm p_2^{k_2})\ldots(\pm p_s^{k_s})$, причём знаки можно комбинировать любым способом так, чтобы знак произведения совпадал со знаком числа n.

§3. Признаки делимости и равноостаточности

Для разложения на множители многозначного числа требуется найти хотя бы небольшие его делители. Для этого предназначены признаки делимости натуральных чисел по их цифрам. Вспомним простейшие признаки делимости и выведем дальнейшие. Пусть дано n-значное натуральное число с десятичной записью $a = \overline{a_{n-1}a_{n-2}...a_1a_0} = 10^{n-1}a_{n-1} + 10^{n-2}a_{n-2} + ... + 10a_1 + a_0$ (a_0 – цифра единиц, a_1 – цифра десятков и т.д.). По смыслу десятичной записи, ***число кратно* 10^k^*, если его последние k цифр равны нулю.***

Сформулируем ***некоторые известные признаки делимости***.

В формулировках последних трёх признаков используются понятия разбиения числа на двузначные или трёхзначные грани – двузначные или трёхзначные числа из цифр данного числа, справа налево (подробнее об этом читайте ниже).

Если…	***то а делится на …***
a_0 *делится на* 2	2
число a_1a_0 *делится на* 4 *или* 25	4 или 25
$a_2\,a_1\,a_0$ *делится на* 8	8
a_0 *равно* 0 *или* 5	5
a_0 *равно* 0	10
сумма цифр делится на 3 *или* 9	3 или 9 соответственно
знакочередующаяся сумма цифр делится на 11	11
сумма двузначных граней делится на 11	
знакочередующаяся сумма трехзначных граней делится на 7,11 *или* 13 *соответственно*	7,11,13 соответственно
сумма трехзначных граней делится на 37	37

Подчеркнём, что ***числа, фигурирующие в левом столбце таблицы, дают такой же, как и а, остаток от деления на соответствующий делитель***.

Первые признаки делимости Вам известны из школы.

Чтобы обосновать *признаки делимости на 3 ина 9, заметим,* что для любого $k = 1, 2, \ldots$ разность $10^k - 1$ кратна девяти. Это видно из десятичной записи этих чисел. В самом деле, $10 - 1 = 9$, $10^2 - 1 = 99$, $10^3 - 1 = 999$ и вообще $10^k - 1 = 99\ldots9$ (k девяток). Данное число можно преобразовать так:

$a = (99\ldots9 + 1)\, a_n + (9\ldots9 + 1)\, a_{n-1} + \ldots + (99 + 1)\, a_2 + (9 + 1)\, a_1 + a_0 =$

$= \underline{9\cdot(11\ldots1\cdot a_n + 1\ldots1\cdot a_{n-1} + \ldots + a_1)} + (a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0)$. Так как подчёркнутое выражение кратно 9 (в частности, трём), то остаток от деления данного числа на 3 или на 9 равен остатку от деления на 3 или соответственно на 9 суммы цифр этого числа.

Займёмся *делимостью на* 11. Для деления на 11 учтём, что $11 = 10 + 1$; из формулы (II) следует, что $10 + 1$, $1000 + 1$, вообще нечётные степени десяти, увеличенные на 1, делятся на 11. Также (в силу формулы (I)) делятся на 11 чётные степени 10, уменьшенные на 1: $100 - 1 = 99$, $10000 - 1 = 9999$ и т.д. Перепишем наше число в виде

$a = a_0 + (11 - 1)a_1 + (99 + 1)\, a_2 + (1001 - 1)\, a_3 + \ldots = a_0 - a_1 + a_2 - a_3 + \ldots + \underline{11a_1 + {}}$ $\underline{+ 99a_2 + 1001a_3 + \ldots}$.

Все подчёркнутые слагаемые кратны 11, поэтому остаток от деления данного числа на 11 равен остатку при делении на 11 знакочередующейся суммы его цифр.

Например, число 1522906 ⋮ 11, так как $6 - 0 + 9 - 2 + 2 - 5 + 1 = 11$ делится на 11.

Рассмотрим разбиение данного числа на двузначные доли – *грани,* начиная справа налево (см. формулировку в таблице). Представим число a в виде $a = \overline{a_1a_0} + 100\overline{a_3a_2} + 100^2\overline{a_5a_4} + \ldots$ и выделим из него сумму $\overline{a_1a_0} + \overline{a_3a_2} + \overline{a_5a_4} + \ldots$:

$$a = \overline{a_1a_0} + \overline{a_3a_2} + \overline{a_5a_4} + \ldots + (99\overline{a_3a_2} + 9999\overline{a_5a_4} + \ldots)$$

Так как $99 = 100 - 1$ делится на 11, то число, взятое в скобки, кратно 11. Тем самым остаток от деления a на 11 равен остатку от деления на 11 суммы его двузначных граней.

Пример 14. Делится ли на 11 число $a = 94317991999$?

Решение. Произведём разбиение числа a на двузначные грани: 9|43|17|99|19|99. Вычислим их сумму: $9 + 43 + 17 + 99 + 19 + 99 = 286$. Не производя деления, подсчитаем сумму двузначных граней полученного числа: $2 + 86 = 88$ – она делится на 11, следовательно, 286 делится на 11, так же, как и данное число.

Признаки делимости на 7 и 13 попробуйте доказать самостоятельно.

Приведём пример применения **объединённого признака делимости на 7, 11, 13.**

Пример 15. Являются ли 7, 11, 13 делителями числа 5159539?

Решение. Разобьём данное число справа налево на трёхзначные числа (грани): 5|159|539 (последняя грань однозначная). Знакочередующаяся сумма полученных чисел равна $539 - 159 + 5 = 385$. Так как $385 = 5 \cdot 7 \cdot 11$ делится на 7 и 11, то данное число делится на 7 и 11, но не делится на 13. Остаток от деления на 13 данного числа такой же, как у 385, т.е. 8.

Аналогично, признак делимости на 37 по трёхзначным граням получается, если учесть, что $1000 = 999 + 1 = 37 \cdot 27 + 1$.

Часто встречаются задачи, где требуется восстановить неизвестные цифры числа, если оно должно делиться на указанные числа.

Пример 16. Найти все пятизначные числа вида $71X1Y$, делящиеся на 132.

Решение. Искомое число должно делиться на попарно взаимно простые числа 3, 4 и 11. Для делимости на 4 необходимо, чтобы двузначное число $1Y$

делилось на 4, откуда $Y = 2$ или 6. Сумма его цифр равна $9 + X + Y$, так что $X + Y \vdots 3$. Знакочередующаяся сумма цифр $Y - 1 + X - 1 + 7 = X + Y + 5$ должна делиться на 11, откуда $X + Y = 6$ или 17, но второй вариант несовместим с делимостью на 3. Следовательно, $Y = 2, X = 4$ или $Y = 6, X = 0$.

Ответ: 71412 и 71016.

§ 4. Вычисление наибольшего общего делителя и наименьшего общего кратного

Сохраним обозначения из параграфа 2. Для натурального числа n запись $n = p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}$ означает каноническое разложение на простые множители.

Рассматривая одновременно два или более чисел, удобно включить в разложение каждого числа все простые делители этих чисел, отсутствующие – в нулевых степенях ($p^0 = 1$ для любого числа p). Например, для $715 = 5\cdot11\cdot13$, $364 = 2\cdot7\cdot13$ можно записать $715 = 2^0\cdot5\cdot7^0\cdot11\cdot13$, $364 = 2^2\cdot5^0\cdot7\cdot11^0\cdot13$.

Пусть $n = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}, m = p_1^{l_1} p_2^{l_2} \ldots p_s^{l_s}$, где $p_1<p_2<\ldots<p_s$, k_i, $l_i \geq 0$ для всех $i = 1, 2, ..., s$. Верны следующие утверждения:

1. НОД(n, m) = $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$, где α_i – меньший из показателей k_i, l_i, $i = 1,\ldots,s$. (IV)

2. НОК(n, m) = $p_1^{\beta_1} p_2^{\beta_2} \ldots p_s^{\beta_s}$, где β_i – больший из показателей k_i, l_i, $i = 1,\ldots,s$. (V)

Пример 17. Доказать, что **НОД(n, m)·НОК(n, m) = nm.**

Решение. НОД(n, m)·НОК(n, m) = $p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} \ldots p_s^{\alpha_s+\beta_s}$, однако для каждого i от 1 до s из пары чисел α_i, β_i одно равно k_i, другое l_i, так что $\alpha_i + \beta_i = k_i + l_i$, откуда НОД($n$, m)·НОК(n, m) = $p_1^{k_1+l_1} p_2^{k_2+l_2} \ldots p_s^{k_s+l_s} = nm$, что и требовалось доказать.

3. *Количество делителей d(n) числа* $n = p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}$ вычисляется по формуле $d(n) = (k_1+1)(k_2+1)\ldots(k_m+1)$. (VI)

В самом деле, любой делитель имеет вид $d = p_1^{l_1} p_2^{l_2} \ldots p_m^{l_m}$, где каждый показатель степени l_i, независимо от остальных, принимает $k_i + 1$ значений, поэтому эти количества надо перемножить. Так, количество делителей числа $496 = 2^4\cdot31$ (пример 13) равно $(4 + 1)(1 + 1) = 10$.

Пример 18. Найти общий вид натуральных чисел, имеющих ровно 2009 делителей.

Решение. По условию, число $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$ имеет, в силу (VI), $d(n) = (k_1 + 1)\dots(k_m + 1) = 2009 = 41 \cdot 7^2$ делителей. Для $d(n)$ есть такие варианты разложения на множители: $2009 = 41 \cdot 49 = 287 \cdot 7 = 41 \cdot 7 \cdot 7$. Соответственно n имеет либо единственный простой делитель с показателем 2008, либо два различных простых делителя с показателями $k_1 = 40, k_2 = 48$ или $k_1 = 6, k_2 = 286$, либо три различных простых делителя с показателями $k_1 = k_2 = 6, k_3 = 40$.

Ответ: $n = p^{2008}$, где p – простое число, либо $n = p_1^{40} p_2^{48}$ или $n = p_1^{6} p_2^{286}$, где p_1, p_2 – различные простые числа, либо $n = p_1^{6} p_2^{6} p_3^{40}$, где p_1, p_2, p_3 – различные простые числа.

Примечание. Из формулы (VI) ясно, что число n, имеющее нечётное число делителей, является квадратом натурального числа, и обратно, так как в этом случае все показатели в каноническом разложении числа n будут чётными.

Понятия наибольшего общего делителя и наименьшего общего кратного легко распространить на любой конечный набор натуральных чисел $a_1, a_2, \dots, a_m$. А именно, натуральное число d называется их наибольшим общим делителем, если оно делит (без остатка) все данные числа и само делится на любой их общий делитель. Натуральное число N называется наименьшим общим кратным чисел $a_1, a_2, \dots, a_m$, если N кратно всем этим числам и делит любое их общее кратное. Правила вычисления НОД и НОК по каноническим разложениям такие же, как и для двух чисел. При этом их можно находить последовательно, пользуясь равенствами

$$\text{НОД}(a_1, a_2, a_3) = \text{НОД}(\text{НОД}(a_1, a_2), a_3) \text{ и}$$

$$\text{НОК}(a_1, a_2, a_3) = \text{НОК}(\text{НОК}(a_1, a_2), a_3).$$

Пример 19. (МГУ, олимпиада «Ломоносов-2007») Натуральные числа *a, b, c* таковы, что НОК(a,b) = 120, НОК(a,c) = 150. Найти НОК(b,c).

Решение. Так как НОК(a,b) = 120 = $2^3 \cdot 3 \cdot 5$, а НОК(a,c) = 150 = $2 \cdot 3 \cdot 5^2$, то, согласно правилу (V), $b \,\vdots\, 2^3 = 8,\ c \,\vdots\, 5^2 = 25$, а, поскольку числа 8 и 25 взаимно простые, то, по свойству 5 делимости, $\text{НОК}(b, c) \,\vdots\, (8 \cdot 25) = 200$. С другой стороны, НОК($a,b,c$) = НОК($a$, НОК($b,c$)) = $2^3 \cdot 3 \cdot 5^2$ = 600 делится на НОК(b,c), следовательно, НОК(b,c) = 200 (это возможно при $b = 2^3 \cdot 5$, $c = 2 \cdot 5^2$, $a = 1$) или НОК(b,c) = 600 (что возможно при $b = 3 \cdot 2^3 \cdot 5$, $c = 5^2$, $a = 3$).

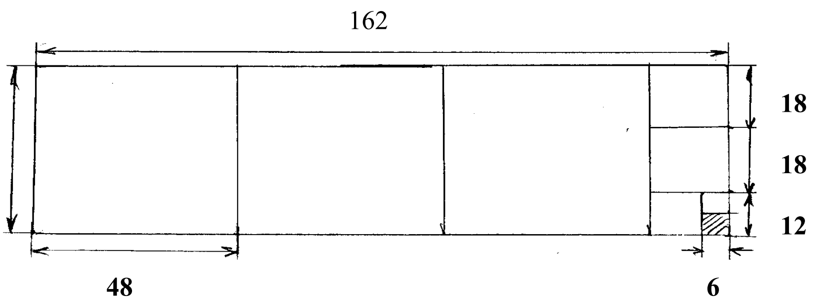
Ответ: НОК(b,c) = 200 или 600.

При решении уравнений в целых числах приходится использовать разложение целых чисел не только на положительные, но и на отрицательные множители. В таком случае каноническим разложением следует считать разложение $n = (\pm p_1^{k_1})(\pm p_2^{k_2})\dots(\pm p_s^{k_s})$, причём знаки можно комбинировать любым способом так, чтобы знак произведения совпадал со знаком числа n.

Чтобы найти НОД двух натуральных чисел a и b, не обязательно знать их разложения на простые множители. Существует иной способ, использующий многократное деление с остатком. Он известен как **алгоритм Евклида.**

Вначале покажем способ на наглядном примере.

Пример 20. От прямоугольника 162мм × 48мм отрезали несколько квадратов со стороной 48 мм, пока не остался прямоугольник, у которого одна сторона короче 48 мм. От полученного прямоугольника отрезают квадраты, у которых сторона равна меньшей стороне прямоугольника, до тех пор, пока это возможно. Чему равна сторона последнего квадрата?



Решение. Начертим заданный прямоугольник.

Откладываем 48 мм на большой стороне прямоугольника. Так как $162 = 3 \cdot 48 + 18$, то получим три квадрата 48 мм × 48 мм и прямоугольник 48 мм × 18 мм ($r_1 = 18$ есть остаток от деления числа 162 на 48). На большей стороне нового прямоугольника откладываем его меньшую сторону: $48 = 2 \cdot 18 + 12$. Получим два квадрата 18 мм ×18 мм и прямоугольник 18 мм × 12 мм ($r_2 = 12$ есть остаток от деления 48 на 18). Этот прямоугольник содержит в себе один квадрат 12 мм × 12 мм и прямоугольник

12 мм × 6 мм, который, в свою очередь, состоит из двух квадратов 6 мм × 6 мм.

Ответ: сторона последнего квадрата равна 6 мм.

Заметим, что длина стороны последнего полученного квадрата есть не что иное, как наибольший общий делитель его сторон, т.к. НОД (162, 48) = 6. И он был найден в результате нескольких делений с остатком (при разрезании прямоугольника на квадраты).

Опишем **алгоритм Евклида**.

Допустим, что $a > b$, и разделим a на b с остатком: $a = bq_0 + r_1$.

Если $r_1 = 0$, то d = НОД(a,b) = b; если $r_1 \neq 0$, то **НОД(*a*,*b*) = НОД(*b*,*r*₁)**. В самом деле, так как a, b делятся на d, то и r_1 делится на d, по свойству 1 делимости. Наоборот, если c делитель b и r_1, то число $a = bq_0 + r_1$ будет делиться на c, т.е. c является общим делителем a и b.

Затем разделим b на r_1: $b = r_1q_1 + r_2$. Если $r_2 = 0$, то НОД (b,r_1) = r_1 = d. В случае $r_2 \neq 0$ получим d = НОД(b,r_1) = НОД(r_1,r_2). Теперь разделим r_1 с остатком на $r_2 < r_1$: $r_1 = r_2q_2 + r_3$ и т.д. Так как после каждого деления числа уменьшаются: $a > b > r_1 > r_2 >$, … то найдётся такой номер k, что $r_{k-2} = r_{k-1}q_{k-1} + r_k$, $r_k \neq 0$, $r_{k-1} = r_kq_k$. На этом процесс закончится, причём d = НОД(a,b) = НОД (r_{k-1}, r_k) = r_k.

Пример 21. Найти НОД(1176, 315).

Решение оформим в виде последовательности делений с остатком.

1176=3·315+231			315=1·231+84			231=2·84+63			84=1·63+**21**			63 = 3·**21**	
a	b	r_1	b	r_1	r_2	r_1	r_2	r_3	r_2	r_3	$\mathbf{r_4}$	r_3	$\mathbf{r_4=d}$

Ответ: НОД(1176, 315) = 21.

Примечание. С помощью алгоритма Евклида

можно найти такие целые числа x, y, что $ax + by = d$ **.**

Покажем это для чисел примера 24. Имеем $d = r_4 = r_2 - r_3$, $r_3 = r_1 - 2r_2$, $r_2 = b - r_1$, $r_1 = a - 3b$. Подставляя эти соотношения, находим $d = r_2 - (r_1 - 2r_2) = 3r_2 - r_1 = 3(b - r_1) - r_1 = 3b - 4r_1 = 3b - 4(a - 3b) = -4a + 15b$.

Окончательно, – 4·1176 + 15·315 = 21.

В следующем примере не обойтись без алгоритма Евклида. Разложить приведённые в нём числа на простые множители вряд ли возможно без математического пакета.

Пример 22. Найти НОД и НОК чисел a = 11…11 (20 цифр) и b = 22…22 (10 цифр).

Решение. Поскольку первое число нечётное, то 2 не является общим делителем данных чисел. Поэтому НОД(a, b) = НОД(a, 1111111111) = 1111111111, так как $\underbrace{11...11}_{20}=\underbrace{11...11}_{10}\cdot\underbrace{10...01}_{11}$.

Ответ: 1111111111 (10 цифр).

Общий делитель приходится искать при исследовании сократимости рациональных дробей целого аргумента.

Пример 23. Определить, на какие натуральные числа может сокращаться дробь $\dfrac{5x-1}{3x+4}$ при целых x.

Решение. Пусть d — общий делитель числителя и знаменателя. Тогда $\begin{cases}5x-1=dk,\\3x+4=dl\end{cases}$ для подходящих целых k, l. Исключим x из этих уравнений:

$\begin{cases}15x-3=3dk,\\15x+20=5dl\end{cases}$ $\Rightarrow d(5l-3k)=23$, а т.к. 23 – простое число, то d = 23.

Ответ: *на* 23.

Замечание. Чтобы найти все значения x, при которых это возможно, требуется решить уравнение $\mathbf{5l-3k=1}$. Решение подобных уравнений в целых числах рассматривается в следующем параграфе.

Историческая сводка. Числа, которые, наподобие числа 496, равны сумме своих собственных делителей, ещё в древности были названы *совершенными.* Первые совершенные числа 6 и 28 были известны в древнем Вавилоне, следующее за 496 совершенное число 8128.

Евклид, живший в 3 веке до н.э. и три тома своего труда «Начала» посвятивший арифметике, доказал, что множество простых чисел бесконечно. Составлять таблицу простых чисел начали ещё древние греки (школа Пифагора, V век до н.э.). По мере накопления простых чисел стало ясно, что никакой общей формулы для их вычисления не существует. Поэтому стали искать формулы, дающие много простых чисел.

Пьер Ферма занимался изучением чисел вида $F=2^m+1$. Такие числа могут быть простыми только при $m=2^k$ (k = 0, 1, 2, ...). В самом деле, если допустить, что $m = 2^k l$, причём число l нечётное, то $F = \left(2^{2^k}\right)^l + 1 = = \left(2^{2^k} + 1\right)\left(2^{2^k-1} - 2^{2^k-2} + \cdots\right)$, по формуле (II). Первые числа Ферма $F_k = 2^{2^k} + 1$: $F_0 = 2$, $F_1 = 2^2 + 1 = 5$, $F_2 = 2^4 + 1 = 17$, $F_3 = 2^8 + 1 = 257$, $F_4 = 2^{16} + 1 = 65537$ являются простыми. Однако больше ни одного простого числа Ферма по сей день не обнаружено, даже с помощью современных компьютеров! Между прочим, числа Ферма участвуют в решении задачи построения правильных многоугольников циркулем и линейкой. Гаусс доказал, что правильный n-угольник только тогда может быть построен, когда разложение n на простые множители имеет вид $n = 2^m \cdot p_1 p_2 \dots p_s$, $m \geq 0, p_1, \dots, p_s$ – различные простые числа Ферма.

Числа вида $2^n - 1$ могут быть простыми лишь при простом n: если $n = mk$, то $2^n - 1$ делится на $2^m - 1$ и $2^k - 1$. Простые числа вида $2^p - 1$ (p – простое число) называют числами Мерсенна и обозначают М(p) (Мерсенн – французский математик, 1588–1648). Наибольшие из известных пока простых чисел являются числами Мерсенна. С 1995 года охота за простыми числами приняла глобальный характер: был создан проект поиска простых чисел с помощью компьютеров, объединённых сетью Интернета (GIMPS – the Great Internet Mersenne Prime Search). С такими огромными числами оказалось возможным работать только благодаря организации взаимодействия сотен тысяч компьютеров (на специальном сайте PrimeNet, http://www.mersenne.org). На сегодняшний день (начало 2010 года) известны 47 простых чисел M(p). 23 августа и 6 сентября 2008 года проверена простота двух очередных чисел Мерсенна, самое большое из них, M(43112609) (№ 45), состоит из 12978189 цифр; более 10 миллионов цифр имеет также число M(37156667) (№ 46). Самое свежее открытие 47-го простого числа Мерсенна произошло 12 апреля 2009 года, в нём 12834064 цифры.

Числа Мерсенна тесно связаны с совершенными числами. Теорема 36 в «Началах» Евклида гласит: если число $n = 2^p - 1$ простое, то число $N = n \cdot 2^{p-1}$ является совершенным. Эту теорему нам сейчас легко доказать. Так как число n простое, то все собственные делители N имеют вид 2^k, где $0 \leq k \leq p-1$, или $n \cdot 2^k$ при $0 \leq k \leq p-2$. Их сумма, согласно формуле (I), равна

$$1 + 2 + \ldots + 2^{p-1} + n \cdot (1 + 2 + \ldots + 2^{p-2}) = \frac{2^p - 1}{2 - 1} + n \cdot \frac{2^{p-1} - 1}{2 - 1} =$$

$$= n \cdot 2^{p-1} + (2^p - 1) - n = N.$$

Леонард Эйлер (1707 – 1783), швейцарский математик, который долгое время работал в Петербурге и прославился трудами по теории чисел, алгебре и другим разделам математики, показал, что любое четное совершенное число можно представить в таком виде. Так что каждое новое простое число Мерсенна даёт и ещё одно совершенное число. Всего известны 52 чётных совершенных числа. Нечётных совершенных чисел до сих пор не открыто, а попытки любителей доказать их отсутствие элементарными средствами воспринимаются специалистами почти как попытки элементарно доказать Великую теорему Ферма.

§ 5. Решение уравнений в целых числах

В решении даже таких простейших уравнений, как линейное уравнение с одним неизвестным, есть свои особенности, если коэффициенты уравнения являются целыми числами, и требуется найти целочисленные решения.

5.1. Линейное уравнение с одним неизвестным $ax = b$ (1), где a, b – целые числа, $a \neq 0$, можно привести к виду, где $a > 0$ (при необходимости умножив обе части на (–1)). Оно имеет единственное целое решение $x = b/a$, если a – делитель b, и не имеет целочисленных решений в противном случае.

Пример 24. Квадратные мраморные плитки были приготовлены, чтобы покрыть прямоугольную площадку размерами $2n + 1$ на $n + 2$ плиток (n – натуральное число). Затем решили использовать эти плитки на площадке шириной $n + 4$ плитки. Возможно ли это, и сколько плиток при этом уложится в ряд?

Решение. Если x – длина ряда плитки, то общее количество плиток равно $x(n+4) = (2n+1)(n+2)$ так что $x = \dfrac{(2n+1)(n+2)}{n+4}$ при условии, что значение дроби равно целому числу. Найдём, при каком n это возможно. Разделим числитель дроби на знаменатель с остатком. Для этого раскроем скобки в числителе: $(2n+1)(n+2) = 2n^2 + 5n + 2$. Положим $t = n + 4$, так что $n = t - 4$, и подставим в выражение числителя:

$$2n^2 + 5n + 2 = 2(t-4)^2 + 5(t-4) + 2 =$$

$$= 2t^2 - 16t + 32 + 5t - 20 + 2 = 2t^2 - 11t + 14.$$

Получим $x = \dfrac{t(2t-11)+14}{t} = 2t - 11 + \dfrac{14}{t} = 2n - 3 + \dfrac{14}{n+4}.$

Число $2n - 3$ целое при натуральном n, поэтому x может быть натуральным, если 14 делится на $n + 4$, а это возможно в двух случаях: при $n + 4 = 7$, $n = 3$, тогда $x = 6 - 3 + 2 = 5$, и при $n + 4 = 14$, $n = 10$, тогда $x = 20 - 3 + 1 = 18$.

Ответ: 7×5 при $n = 3$ или 14×18 при $n = 10$.

Уравнения в целых числах с двумя и более неизвестными рассматривал в своем произведении «Арифметика» Диофант (III в н. э.). В его честь целочисленные уравнения обычно называют диофантовыми. Самое известное из них:

– 5.2. Линейное уравнение с двумя неизвестными: $ax + by = c$ (2), где a, b, c – данные целые числа, причём $ab \neq 0$ (иначе это уравнение с одним неизвестным).

Пример 25. Показать, что любую сумму (в рублях), кроме 1 и 3 рублей, можно заплатить монетами по 2 и 5 рублей, а если допустить сдачу (теми же монетами) – то вообще любую.

Решение. Пусть требуется заплатить n рублей x монетами по 2 рубля и y монетами по 5 рублей (x, y – целые числа, отрицательное значение x или y указывает, что получена сдача), тогда составим уравнение $2x + 5y = n$. Если $(x; y)$ решение, то $x = \dfrac{n-5y}{2}$, $n - 5y$ должно делиться на 2. Ввиду взаимной простоты 2 и 5, это будет выполнено, если y одинаковой чётности с n. При $n = 1$ или 3 подойдёт $y = -1$, $x = 3$ или 4 соответственно (т.е. заплатить 3 или 4 монеты по 2 рубля и взять сдачу 5 рублей), при $n = 2k$ достаточно $y = 0$, $x = k$. Если же $n \geq 5$ нечётное, можно взять $y = 1$, тогда получим $x \geq 0$.

Возвращаясь к общему случаю, найдём, при каких условиях на коэффициенты уравнение (2) может иметь целочисленное решение.

Например, уравнение $2x - 4y = 21$ не имеет решений, так как левая часть делится на 2, а правая не делится.

Теорема. ***Уравнение* (2) *тогда и только тогда имеет целочисленное решение* ($x; y$), *когда с делится на НОД*(a, b).**

Это условие выполнено, если a и b взаимно простые, как было в примере 26.

Допустим, что **НОД(a, b) = d,** так что $a = da_1, b = db_1,\ c = dc_1$, причём a_1 и b_1 взаимно простые. Разделив уравнение (2) на d, получим уравнение $a_1x + b_1y = c_1$ с взаимно простыми a_1, b_1.

Найти хотя бы одно решение уравнения $ax + by = c$ с взаимно простыми a, b можно методом, применённым при решении примера 26: выразить y через x или наоборот: $y = \dfrac{c - ax}{b}$. Так как **НОД(a, b) = 1,** то найдутся такие целые числа u, v, что $au + bv = 1$ (см. примечание к алгоритму Евклида после примера 22). Умножив обе части уравнения на c, получим $auc + bvc = c$, так что уравнение имеет хотя бы одно решение $x_1 = uc,\ y_1 = vc$. Это показывает, что найдётся целое значение x_0, при котором $y_0 = \dfrac{c - ax_o}{b}$ также будет целым. Пара $(x_0; y_0)$ будет решением уравнения (2).

Зная одно (так называемое «частное») решение, можно найти все решения уравнения $ax + by = c$ с взаимно простыми a, b. Пусть $(x; y)$ – произвольное решение, а $(x_0; y_0)$ – частное решение. Вычтем почленно из равенства $ax + by = c$ равенство $ax_0 + by_0 = c$, получим $a(x - x_0) + b(y - y_0) = 0$, т.е. $X = x - x_0,\ Y = y - y_0$ – решение

соответствующего однородного уравнения $aX + bY = 0$ **(3).**

Перенесём bY в правую часть равенства (3): $aX = -bY$. Так как X, Y целые числа, то aX делится на b; по свойству 5 делимости, X делится на b, в силу взаимной простоты a, b, т.е. $X = bt$ для подходящего целого t, откуда $Y = -at$. Итак, любое решение уравнения (2) находится по формулам

$$\begin{cases} x = x_0 + bt \\ y = y_0 - at,\ t \in Z \end{cases} \tag{4}$$

Пример 26. Найти все целочисленные решения уравнения $5l - 3k = 1$ (это уравнение встретилось в примере 26).

Решение. Выразим, например, k через l: $k = \dfrac{5l - 1}{3}$. Сразу видно, что при $l = 2$ получим $k = 3$; мы нашли частное решение $l_0 = 2$, $k_0 = 3$. Теперь запишем $5l - 3k = 5 \cdot 2 - 3 \cdot 3,\ 5(l - 2) - 3(k - 3) = 0.$ Нам остается решить однородное уравнение $5X - 3Y = 0,\ 5X = 3Y$, где $X = l - 2, Y = k - 3$. Так как числа 5 и 3 взаимно простые, отсюда следует, что X делится на 3, а Y делится на 5, так что $X = 3t, Y = 5t, t \in \mathbb{Z}$. Окончательно, $\begin{cases} l = 2 + 3t \\ k = 3 + 5t,\ t \in Z \end{cases}$.

Примечание. Тем самым мы нашли все x, удовлетворяющие требованию примера 20: $5x = 1 + dk = 1 + 23(3 + 5t) = 70 + 23 \cdot 5t, x = 14 + 5t, t \in Z$.

5.3. Примеры решения нелинейных уравнений

Уравнения $P = c$, где P – многочлен с целыми коэффициентами от одной или нескольких неизвестных и *без свободного члена*, а c – целое число, часто решают, разлагая левую и правую части на множители с целыми коэффициентами и используя единственность разложения из основной теоремы арифметики.

Пример 27. Найти все целые корни уравнения $x^3 - 4x = 15$.

Решение. Левую часть разложим на множители: $x^3 - 4x = x(x^2 - 4) = (x - 2)x(x + 2) = 15$. В разложении числа 15 на три различных сомножителя обязательно участвует 1. Возможны варианты: $x - 2 = 1$, $x = 3$, $x + 2 = 5$ или $x - 2 = -5$, $x = -3$, $x + 2 = -1$, но тогда произведение равно – 15. Значит, других целых корней это уравнение не имеет.

Ответ: $x = 3$.

Пример 28. Найти все решения уравнения $4x^2 - y^2 = -4$ в целых числах.

Решение. Разложим левую часть уравнения на множители:

$4x^2 - y^2 = (2x - y)(2x + y)$. $4x^2 - y^2 = (2x - y)(2x + y) = -4$. Так как x и y – целые числа, то $(2x - y)$, $(2x + y)$ также целые числа, произведение которых равно – 4. Таким образом, получаем 6 систем уравнений, различающихся только правыми частями. Поэтому запишем все их вместе:

$$\begin{cases} 2x - y = -1; \quad 1; -4; \quad 4; \quad 2; -2 \\ 2x + y = \quad 4; -4; \quad 1; \ -1; -2; \quad 2 \end{cases},$$
(правые части уравнений, соответствующих каждому случаю, расположены одна под другой).

Сложив уравнения, получим соответственно

$$\begin{cases} 4x = 3; \qquad -3; \qquad -3; \qquad 3; \qquad 0; \qquad 0 \\ y = \quad 4 - 2x; \ -4 - 2x; 1 - 2x; \ -1 - 2x; -2 - 2x; \ 2 - 2x \end{cases}.$$

Лишь в последних двух случаях x будет целым, следовательно, уравнение имеет два решения: $x = 0$, $y = -2$ и $x = 0$, $y = 2$.

Ответ: (0; – 2), (0; 2).

Бывает, что многочлен, стоящий в левой части уравнения, не удаётся разложить на множители, но одна из неизвестных входит в уравнение в первой степени. Тогда целесообразно выразить её через другую неизвестную (как это часто делают при решении систем алгебраических уравнений).

Пример 29. (МФТИ, 1998) Решить в целых числах уравнение

$$x^3 - xy - 7x + 2y + 23 = 0.$$

Решение. В уравнение y входит в первой степени, поэтому выразим y через x: $x^3 + y(2-x) - 7x + 23 = 0$, $y = \dfrac{x^3 - 7x + 23}{x-2}$. Чтобы легче разделить числитель на знаменатель, введём $t = x - 2,\ x = t + 2, x^3 = t^3 + 6t^2 + 12t + 8$,

$y = \dfrac{t^3 + 6t^2 + 12t + 8 - 7t - 14 + 23}{t} = t^2 + 6t + 5 + \dfrac{17}{t}$. По условию, t и y целые, поэтому 17 должно делиться на t. Таким образом, возможны варианты: $t = 1$, $x = 3$, $y = 29$; $t = -1$, $x = 1$, $y = -17$; $t = 17$, $x = 19$, $y = 397$; $t = -17$, $x = -15$, $y = 191$.

Ответ: (3; 29), (1; – 17), (19; 397), (– 15; 191).

Уравнение, решенное в примере 30 – это частный случай уравнения второго порядка $ax^2 + bxy + cy^2 = d$ **(4)** с целыми a, b, c, d.

Оказывается, некоторые из них можно решить и в тех случаях, когда левую часть нельзя разложить на множители первой степени с целыми коэффициентами.

§ 6. Несколько более сложных задач об остатках

Идеи, связанные с изучением остатков, которые использовались выше, например, при решении задач на делимость, уравнений в целых числах или обсуждении признаков делимости, можно развить. Соответствующий раздел теории чисел называется теорией сравнений. Эти сравнения выходят за рамки нашего задания (интересующиеся могут обратиться к книгам и статье [2,5,7,9] из списка литературы). Однако мы разберем несколько задач, используя рассмотрение остатков.

Начнём с подготовительного примера.

Пример 30. Найти остатки от деления на 3 чисел вида $2n^2 + 1$ для всевозможных натуральных чисел n.

Решение. Если n делится на 3, то остаток от деления на 3 равен 1, как видно из определения деления с остатком.

Допустим, n не делится на 3. В этом случае n имеет вид $n = 3k \pm 1 \Rightarrow n^2 = 9k^2 \pm 6k + 1$, $2n^2 + 1 = 18k^2 \pm 12k + 3$, так что число $2n^2 + 1$ делится на 3.

Ответ: Остаток равен 1, если n кратно 3, и 0, если n не кратно 3.

Пример 31. Найти все простые числа p, для которых число $2p^2 + 1$ простое.

Решение. Из примера 35 вытекает, что для всех простых чисел $p > 3$ число $2p^2 + 1$ делится на 3, т.е. является составным. Следовательно, число $2 \cdot 3^2 + 1 = 19$ – единственное простое число вида $2p^2 + 1$.

Ответ: $p = 3$.

Чтобы узнавать остатки от деления степеней натуральных чисел, полезно решить следующую задачу.

Задача 32. Пусть a, m – целые числа и $a = r + mq$ (q целое). Доказать, что для любого натурального числа k верно равенство $a^k = r^k + ms$, где число s целое.

Решение. Применим метод математической индукции.

Для $k = 1$ утверждение верно по условию. Допустим, что для некоторого натурального числа k равенство $a^k = r^k + ms$ верно.

Тогда $a^{k+1} = (r + mq)(r^k + ms) = r^{k+1} + m(qr^k + rs + mqs)$. Согласно принципу индукции, равенство верно для всех $k = 1,2,\ldots$

Пример 33. Выяснить, существует ли такое натуральное число n, что $2011^{2011} + 2009^{2010} = n^2$.

Решение. Будем рассматривать остатки от деления на 3. Так как 2010 делится на 3, то $2010 = 3q$ (q натуральное), поэтому $2011 = 1 + 3q$, $2009 = -1 + 3q$. Отсюда с помощью задачи 37 получаем: $2011^{2011} = 1^{2011} + 3s = 1 + 3s$ и $2009^{2010} = (-1)^{2010} + 3t = 1 + 3t$ (s, t целые). Следовательно,

$$2011^{2011} + 2009^{2010} = 2 + 3(s + t) = 2 + 3u, u = s + t.$$

Допустим, что $2011^{2011} + 2009^{2010} = n^2$ для некоторого натурального n, тогда $2n^2 + 1 = 2(2 + 3u) + 1 = 3(2u + 1) + 2$. Это противоречит результату примера 35.

Ответ: такое натуральное число не существует.

В заключение приведём без доказательства теорему, полезную при решении задач на делимость степеней. Она известна как *малая теорема Ферма.*

Малая теорема Ферма. Пусть p — простое число, a — натуральное число. Если a не делится на p, то $a^{p-1} - 1$ делится на p (то есть $a^{p-1} = 1 + pq$, q натуральное).

Пример 34. Показать, что число $n^{13} - n$ делится на 13 при любом натуральном n.

Решение. Если n кратно 13, то данное утверждение очевидно. Допустим, что n не делится на 13. По малой теореме Ферма для $p = 13$ получим, что число

$n^{12} - 1$ делится на 13, следовательно, $n^{13} - n = n(n^{12} - 1)$ также делится на 13, что и требовалось доказать.

Решим следующую задачу при помощи малой теоремы Ферма.

Пример 35. Доказать, что число $216^{321} + 321^{216}$ делится на 7.

Решение. Так как $p = 7$ простое число, то, согласно малой теореме Ферма, $216^6 = 1 + 7q, 321^6 = 1 + 7s$. Разделим 321 на 6: 321 = 53· 6 + 3 и применим результат задачи 37: $216^{321} = (216^6)^{53} \cdot 216^3 = (1 + 7t) \cdot 216^3$

$216^6 \equiv 1(mod7)$ и $321^6 \equiv 1\ (mod7)$. Кроме того, $216=217 - 1 = 7\cdot 31 - 1 \Rightarrow$ $216^3 = 7u - 1$ и $216^{321} = (1 + 7t) \cdot (7u - 1) = 7(u - t + ut) - 1 = 7w - 1$.

Далее, $216 = 6\cdot 36$, поэтому $321^{216} = (321^6)^{36} = (1 + 7s)^{36} = 1 + 7v$ (mod 7).

Складывая равенства $216^{321} = 7w - 1$ и $321^{216} = 1 + 7v$, получаем $216^{321} + 321^{216} = 7(v + w)$, что и требовалось доказать.

Следующую задачу также можно решить при помощи малой теоремы Ферма, хотя на вступительном экзамене, разумеется, этого не предполагалось.

Пример 36. (МФТИ, 2002) Найти последнюю цифру и остаток от деления числа $a = 3^{2002} + 7^{2002}$ на 11.

Решение. Последние цифры последовательных степеней натурального числа периодически повторяются, причём период не превосходит количества десятичных цифр, т.е. 10. Установим это экспериментально; при подсчётах на каждом шаге достаточно умножать только последнюю цифру предыдущего произведения. Убедимся, что у чисел 3^k и 7^k последние цифры переодически повторяются: $3^1 = \underline{3}, 3^2 = 9, 3^3 = 27, 3^4 = 81, 3^5 = 24\underline{3}, \ldots$

$$7^1 = \underline{7}, 7^2 = 49, 7^3 = 343, 7^4 = 2401, 7^5 = 1680\underline{7}.$$

В обоих случаях последние цифры повторяются с периодом 4, а т.к. 2002 = 4 · 500 + 2, то легко насчитать, что последние цифры у обеих степеней 9, а их у суммы – 8.

Остатки степеней числа a при делении на p также периодически повторяются, причём период не превосходит p –1.

Убедитесь, что период остатков при делении на 11 для основания 3 равен 5, а для основания 7 равен 10.

Значит, у 3^{2002} остаток от деления на 11 такой же, как у 3^2, т.е. 9, а у 7^{2002} такой же, как у 7^2, т.е. 5, а у их суммы такой же, как у 9 + 5 = 14, т.е. 3.

Ответ: последняя цифра 8, остаток 3.

Рекомендуемая литература

1. Агаханов Н.Х., Подлипский О.К. Математические олимпиады Московской области 1993-2005. Изд.2.– М.: МФТИ, 2006.
2. Алфутова Н. Б., Устинов А. В. Алгебра и теория чисел. Сборник задач для математических школ. 2-е издание.– М: МЦНМО, 2005.
3. Виленкин Н.Я., Шибасов Л.П., Шибасова З.Ф. За страницами учебника математики, 10 – 11. – М.: Просвещение, 1996.
4. Галкин В.Я., Сычугов Д.Ю., Хорошилова Е.В. Конкурсные задачи, основанные на теории чисел. – М.: Макс Пресс, 2003.
5. Математическая энциклопедия абитуриента, вып. 1: Петрович А.Ю., Сидоров Ю.В., Шабунин М.И. Числа и многочлены. М.: МФТИ и РОУ, 1992.
6. Фалин Г.И., Фалин А.И. Алгебра на вступительных экзаменах по математике в МГУ. – М.: БИНОМ. Лаборатория знаний, 2006.
7. Чубарова Е.И., Чубаров И.А. Элементы теории сравнений и их применение к решению задач. – «Потенциал», 2005, № 8, с. 17 – 27.
8. Шень А. Простые и составные числа. – М.: МЦНМО, 2005.
9. Шибасов Л.П. От единицы до бесконечности.– М.: Дрофа, 2006.

Контрольные вопросы

(*числа* n, m *натуральные,* a, b *целые*)

1(1). Пусть число a делится на n, а b не делится на n. Может ли $a+b$ делиться на n?

2(1). Пусть числа a, b не делятся на n. Верно ли, что $a-b$ не делится на n?

3(2). Сумма и произведение чисел a и b делятся на n. Что можно сказать о делимости чисел a и b на n, если число n: а) простое, б) составное?

4(2). Натуральные числа m, n таковы, что НОД(m,n)+НОК$(m,n)=m+n$. Докажите, что одно из этих чисел является делителем другого.

5(2). Найдите НОД чисел 3333333333 и 11…11 (во втором числе 2010 цифр).

6(2). Докажите, что если n не делится на 5, то его квадрат, уменьшенный или увеличенный на 1, делится на 5.

Задачи

1(3). При перемножении двух натуральных чисел произведение было ошибочно увеличено на 372. При делении полученного (неверного) произведения на меньший сомножитель получилось в частном 90, в остатке 29. Найдите эти числа.

2(5). Докажите, что при любом целом значении n выражение:

(а)(2) $(n^2-5n+3)^2-9$ делится на 24;

(б)(3) $2n^6-n^4-n^2$ делится на 36.

3(3). Найдите все пятизначные числа вида $\overline{5X76Y}$ (X, Y – цифры), делящиеся на 44.

4(4). Найдите все такие двузначные числа, у которых сумма квадратов цифр на 97 меньше удвоенного числа.

5(7). Докажите, что при любом натуральном n

(а)(3) $5^{2n+1}+3^{n+2}\cdot 2^{n-1}$ делится на 19;

(б)(4) $5^{5n+1}+4^{5n+2}+3^{5n}$ делится на 11.

6(3). Найдите все целые значения n, при которых числа $n-2$, $n+12$, $n+26$ являются простыми.

7(2). На какие натуральные числа можно сократить дробь $\dfrac{3n-7m}{2n+m}$ при целых, взаимно простых n, m?

8(12). Решите в целых числах уравнения:

(а)(2) $7x-4y=107$;

(б)(3) $3x^2+5xy+2y^2=7$;

(в)(3) $3xy+14x+17y+71=0$;

9(4). Докажите, что при любом простом $p>3$ число $10p^2-3p+2$ составное.