Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение дополнительного образования детей
«Заочная физико-техническая школа
Московского физико-технического института
(государственного университета)»

МАТЕМАТИКА

Элементы теории чисел

(факультативное)

Задание №6 для 11-х классов

(2013 – 2014 учебный год)

г. Долгопрудный, 2014

Составитель: Е.Г. Молчанов, ассистент кафедры высшей математики МФТИ.

Математика: задание №6 для 11-х классов (2013 – 2014) учебный год), 2014, 28 с.

Дата отправления заданий по физике и математике – 12 апреля 2014 г.

Внимание! Данное задание является факультативным, т. е. присылать его в ЗФТШ на проверку не обязательно, но мы настоятельно рекомендуем Вам внимательно проработать его, т. к. задачи по темам «Теория чисел» и «Комбинаторика» были включены в 2012 году в олимпиаду «Физтех-2012».

Составитель:
Молчанов Евгений Геннадьевич
Подписано 18.02.14. Формат 60×90 1/16.
Бумага типографская. Печать офсетная. Усл. печ. л. 1,75.
Уч.-изд. л. 1,55. Тираж 600. Заказ №49-з.

Заочная физико-техническая школа
Московского физико-технического института
(государственного университета)

ООО «Печатный салон ШАНС»

Институтский пер., 9, г. Долгопрудный, Москов. обл., 141700.
ЗФТШ, тел./факс (495) 408-51-45 – **заочное отделение,**
тел./факс (498) 744-63-51 – **очно-заочное отделение,**
тел. (499) 755-5580 – **очное отделение.**

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

Наш сайт: www.school.mipt.ru

Введение

Действия с натуральными и целыми числами знакомы вам с младших классов, когда математика сводится по существу к арифметике. 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. Всё большую популярность такие задачи приобретают на олимпиадах, проводимых МФТИ, МГУ и другими вузами, а также присутствуют в ЕГЭ по математике (задание С6). Рекомендованные пособия помогут вам в их решении и более глубоком изучении темы.

§1. Делимость целых чисел

1.1. Основные понятия и факты

Напомним основные понятия и факты.

Множество натуральных чисел обозначается символом $\mathbb{N}$.

Множество целых чисел обозначается символом $\mathbb{Z}$.

Множество рациональных чисел обозначается символом $\mathbb{Q}$.

Множество действительных чисел обозначается символом $\mathbb{R}$.

В дальнейшем, если не будет сказано иного, мы будем рассматривать только множества целых и натуральных чисел.

Натуральное число n называется *делителем* целого числа m, если для подходящего целого числа k верно равенство: $m = nk$. В этом случае говорят, что m делится на n и обозначают как «$m \vdots n$». Число m называют кратным числу n.

Например, $117 \vdots 9$ $(117 = 13 \cdot 9)$; $91 \vdots 7$ $(91 = 13 \cdot 7)$.

Число $p \geq 2$ называют *простым*, если оно делится только на себя и на единицу. Множество простых чисел обозначают символом $\mathbb{P}$. *Составными числами* называют целые числа, имеющие больше двух различных делителей.

Например, 17 – простое число, а $153 = 17 \cdot 9$ – составное.

Натуральное число k называют *общим делителем* чисел m, n если $m \vdots k$ и $n \vdots k$. Наибольшее такое число k называют *наибольшим общим делителем* m и n и обозначают как НОД(m, n) (иногда просто (m, n)). Если наибольший общий делитель двух чисел равен единице, эти числа называют *взаимно простыми*.

Например, 2 – общий делитель чисел 12 и 8, 4 – наибольший общий делитель чисел 12 и 8, т. е. НОД $(12,8) = 4$.

Целое число k называют *общим кратным* чисел m и n, если $k \vdots m$ и $k \vdots n$. Наименьшее натуральное число, кратное m и n называют *наименьшим общим кратным* m и n и обозначают как НОК(m,n).

Например, 120 – общее кратное чисел 12 и 8, 24 – наименьшее общее кратное чисел 12 и 8, т. е. НОК $(12{,}8) = 24$.

Напомним основные свойства делимости.

Свойство 1. Если целое число m делится на число n, а число n делится на число k, то число m делится на число k.

Свойство 2. Если k – общий делитель целых чисел m и n, то:

1. $m + n$, $m - n$ делятся на k;
2. mn делится на k (точнее – на k^2).

Следствие свойства 2. Если одно из чисел m или n делится на k, а второе не делится на k, то $m + n$, $m - n$ не делятся на k.

Действительно, если m делится на k и, например, $m + n$ делится на k (от противного), то $n = (m + n) - n$ также бы делилось на k согласно свойству 2.

Свойство 3. Если целое число a делится на взаимно простые делители m и n, то a делится на mn.

Свойство 4. Если ab (a, b – целые) делится на простое число p, то a или b делится на число p.

Свойство 5. Если ab делится на число n и a взаимно просто с числом n, то b делится на число n.

1.2. Разложение на простые множители. Основная теорема арифметики

Сформулируем *основную теорему арифметики*:

Любое натуральные число n, большее единицы, можно разложить в произведение простых чисел. Это разложение единственно, с точностью до порядка следования сомножителей.

Приведём набросок доказательства первой части этой теоремы. Заметим, что если число $n > 1$ не простое, оно должно иметь более двух различных делителей. С учётом того, что $n \vdots n$ и $n \vdots 1$, должен существовать ещё хотя бы один делитель числа n – число a, $1 < a < n$. Таким образом, или n само является простым числом (и разложение получено), или оно раскладывается в произведение $n = ab$, $1 < a < n$, $1 < b < n$. Каждое из чисел a и b также или является простым, или раскладываются далее в произведение ещё более меньших чисел, не равных единице. Данный процесс разложения не может продолжаться бесконечно, и в итоге число n будет представлено в виде произведения простых чисел.

Строгое доказательство того, что такое разложение единственно с точностью до порядка следования сомножителей, первым дал немецкий математик К.Ф. Гаусс (1777 – 1855), внесший крупный вклад в развитие многих областей математики.

Пример 1. Найти все простые числа, не превосходящие 100.

Решение. Для нахождения таких чисел удобно воспользоваться методом, известным как «решето Эратосфена». Этот метод назван в честь греческого математика Эратосфена, жившего в III в. до н. э., и заключается в следующем. Выпишем все числа от 1 до 100 в таблицу:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100

Далее, число 1 вычеркнем (оно не простое), числа 2 и 3 оставим как простые и вычеркнем все числа, кратные 2 и 3.

	2	3		5		7				11		13				17		19	
		23		25				29		31				35		37			
41		43				47		49				53		55				59	
61				65		67				71		73				77		79	
		83		85				89		91				95		97			

Далее, оставим число 5 как простое и вычеркнем все числа, кратные 5. Затем то же самое сделаем с числом 7.

	2	3		5		7				11		13				17		19	
		23						29		31						37			
41		43				47						53						59	
61						67				71		73						79	
		83						89								97			

Все оставшиеся числа будут простые. Это связано со следующим свойством:

Если число $n = ab$, то хотя бы один из сомножителей не превосходит $\sqrt{n}$.

Действительно, если предположить противное, т. е. предположить, что $a > \sqrt{n}$ и $b > \sqrt{n}$, то $ab > \sqrt{n} \times \sqrt{n} = n$ и возникает противоречие.

В примере мы проверили все простые делители, не превосходящие $\sqrt{100} = 10$. Таким образом, любое составное число, меньшее 100, делится на 2, 3, 5 или 7.

Во времена Эратосфена писали на восковых дощечках, а вместо того, чтобы числа вычёркивать, дощечку прокалывали, так что в итоге она становилась похожей на решето. Отсюда и произошло название метода.

Ответ: простые числа, меньшие 100, представлены в третьей таблице.

Итак, для нахождения делителей числа n можно воспользоваться следующим **способом**.

Проверим в порядке возрастания делимость числа n на простые числа, не превосходящие $\sqrt{n}$. Если ни на какое из таких чисел n не делится, то n – простое. Иначе, запишем $n = pm$ и будем далее искать делители числа m по тому же правилу.

Пример 2. Разложите на простые множители число 76557.

Решение. Начнём проверять делимость числа 76557 на простые числа, расположенные в порядке возрастания. На 2 число 76557 не делится, зато делится на 3: $76557 = 3 \times 25519$. Теперь, будем искать делители числа 25519. Это число не делится на 2, 3, 5, 7, 11, зато делится на 13: $25519=1963\times13$. Число 1963 также делится на 13, т. е. $25519=151\times13^2$. Посмотрим на число 151. Заметим, что $151<169=13^2$, значит, если число 151 раскладывается на множители, один из этих множителей будет меньше 13. Но все простые числа, меньшие 13, уже были проверены. Значит, число 151 простое и $76557=3\times13^2\times151$.

Ответ: $76557=3\times13^2\times151$.

Пример 3. Докажите, что число $2n^4 - 11n^2 - 6$ является составным при всех целых n.

Решение. Разложим этот многочлен на множители, решив для этого уравнение $2t^2 - 11t - 6 = 0$. Его корни: 6 и $-\frac{1}{2}$. Отсюда $2t^2 - 11t - 6 = (t-6)(2t+1)$ и, следовательно, $2n^4 - 11n^2 - 6 = (n^2-6)(2n^2+1)$.

Таким образом, мы получили разложение целого числа $2n^4 - 11n^2 - 6$ на два целых числа: $(n^2 - 6)$ и $(2n^2 + 1)$. Если ни одно из этих чисел по модулю не равно единице, то исходное число является составным. Равенства $n^2 - 6 = 1$; $n^2 - 6 = -1$; $2n^2 + 1 = -1$ невозможны, равенство $2n^2 + 1 = 1$ возможно при $n = 0$, но при $n = 0$ число $2n^4 - 11n^2 - 6 = -6$ является составным.

Пример 4. Разложите на два сомножителя число $2^{16} + 2^8 + 1$.

Решение. Заметим, что если слагаемое 2^8 в исходном числе домножить на 2, получится формула суммы квадратов: $2^{16} + 2 \times 2^8 + 1 = (2^8 + 1)^2$. Тогда добавим и вычтем число 2^8 в исходную формулу, получив: $2^{16} + 2^8 + 1 + 2^8 - 2^8 = (2^8 + 1)^2 - 2^8$. Последнее выражение можно разложить как разность квадратов: $(2^8+1)^2-2^8=$ $=(2^8+1+2^4)(2^8+1-2^4)$.

Ответ: $2^{16}+2^8+1$=$(2^8+2^4+1)(2^8-2^4+1)$.

1.3. Каноническое разложение числа. Нахождение количества делителей

Вернёмся к основной теореме арифметики (см. п. 1.2.)

Если в разложении натурального числа n, большего единицы, встречаются одинаковые простые числа, их удобно группировать в степени. В результате получается:

$$n=p_1^{k_1}p_2^{k_2}\dots p_m^{k_m},$$

где $p_1,p_2,\dots,p_m$ – различные простые числа. Если потребовать, чтобы $p_1<p_2<\dots<p_m$, то такое разложение будет абсолютно однозначным. Это разложение называется **каноническим.**

Например, $31752=2^3\cdot 3^4\cdot 7^2$.

Зная каноническое разложение, можно найти **все делители числа** n. Они имеют вид $d=p_1^{l_1}p_2^{l_2}\dots p_m^{l_m}$, где каждый показатель степени l_i может принимать значение от 0 до k_i.

Пример 5. Найти все делители числа 28.

Решение. Разложим число 28 в канонический вид: $28=2^2\times 7$. Таким образом, в разложении каждого из делителей числа 28 может присутствовать только двойка в степени не более двух, а также семёрка в степени не более единицы. Выпишем все делители в таблицу:

$2^0\times 7^0=1$	$2^1\times 7^0=2$	$2^2\times 7^0=4$
$2^0\times 7^1=7$	$2^1\times 7^1=14$	$2^2\times 7^1=28$

Ответ: делители числа 28 суть 1, 2, 4, 7, 14 , 28.

Заметим, что если сложить все делители числа 28, кроме него самого, мы получим $1+2+4+7+14=28$, т. е. исходное число. Числа, равные сумме своих меньших самого числа делителей, называются *совершенными*. Таким образом, 28 – совершенное число.

Зная каноническое разложение, можно найти количество всех делителей числа. Действительно, пусть $n=p_1^{k_1}p_2^{k_2}\dots p_m^{k_m}$. Делители такого числа имеют вид $d=p_1^{l_1}p_2^{l_2}\dots p_m^{l_m}$, где каждый показатель степени l_i можно выбрать независимо (k_i+1) способом (от 0 до k_i). Все эти числа надо перемножить. Таким образом, **количество делителей** числа $n=p_1^{k_1}p_2^{k_2}\dots p_m^{k_m}$ равняется

$$d(n)=(k_1+1)\times(k_2+1)\times\dots\times(k_m+1).$$

Следствие: число имеет нечётное количество делителей, только если это число является квадратом.

Действительно, нечётное количество делителей, равносильно тому, что каждый сомножитель в формуле для $d(n)$ нечётен, значит все числа $k_1+1, k_2+1, \dots, k_m+1$ – нечётны, и вхождение каждого простого числа в n чётно. Это означает, что n является полным квадратом.

1.4. Нахождение НОД и НОК

Запишем каноническое разложение чисел m и n: $n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$, $m = p_1^{l_1} p_2^{l_2} \dots p_s^{l_s}$. Вообще-то говоря, входящие в состав разложения m и n простые числа могут быть разными, например $n = 15 = 3^1 \times 5^1$, $m = 10 = 2^1 \times 5^1$. В таком случае дополним разложение каждого числа «недостающими» простыми числами в нулевой степени. В этом же примере, $15 = 2^0 \times 3^1 \times 5^1$, $\quad 10 = 2^1 \times 3^0 \times 5^1$.

Итак, $n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$, $m = p_1^{l_1} p_2^{l_2} \dots p_s^{l_s}$, где $p_1 < p_2 < \dots < p_s$ и $k_i, l_i \geq 0$ для всех i от 1 до s. В таком случае можно записать явные формулы НОД(m,n) и НОК(m,n):

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

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

Также стоит отметить следующее свойство НОК и НОД:

3. НОД$(m,n)\times$ НОК(m,n)=mn.

Это свойство следует из того, что сумма меньшего и большего из двух показателей равна сумме обоих этих показателей, взятых в произвольном порядке.

Пример 6. Найдите НОД (30, 25).

Решение. Запишем канонические разложения чисел 30 и 25 и дополним их «недостающими» простыми числами.

$30 = 2^1 \cdot 3^1 \cdot 5^1$; $25 = 2^0 \cdot 3^0 \cdot 5^2$.

По формуле 1 (выше) получим: НОД$(30{,}25) = 2^0 \cdot 3^0 \cdot 5^1 = 5$.

Ответ: 5.

§2 Десятичная запись числа

Всякое натуральное число N единственным образом представимо в десятичной записи, которая имеет вид

$$N = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0,$$

где n – натуральное число или 0, а $a_n, a_{n-1}, \cdots, a_2, a_1, a_0$ – цифры от 0 до 9, $a_n \neq 0$. Для краткости это число также записывают в виде

$$N = \overline{a_n a_{n-1} \dots a_2 a_1 a_0}.$$

Крышка сверху ставится, чтобы отличить десятичную запись числа от произведения цифр $a_n \cdot a_{n-1} \cdot ... \cdot a_2 \cdot a_1 \cdot a_0$.

Число M называется $m -$ значным в том и только в том случае, если верно неравенство $10^{m-1} \leq M < 10^m$.

Пример 7. Незнайка перемножил все цифры какого-то натурального числа, и получил 2013. Докажите, что Незнайка ошибся.

Решение. Разложим 2013 на простые множители. $2013 = 3 \cdot 11 \cdot 61$. Число 61 является простым, и, согласно свойству 4 делимости, если произведение чисел делится на 61, какое-то число должно также делиться на 61. Однако, цифры $1, \dots, 9$ нацело на 61 не делятся, а если среди цифр этого натурального присутствует 0, то и произведение всех цифр также равно 0. Противоречие.

Пример 8. («Физтех-2012») Последнюю цифру шестизначного числа переставили на первое место и полученное число вычли из исходного числа. Какие числа из промежутка $[618222; 618252]$ могли получиться в результате вычитания?

Решение. Пусть шестизначное число N имеет десятичную запись $\overline{a_5a_4a_3a_2a_1a_0}$. Для удобства обозначим $B = \overline{a_5a_4a_3a_2a_1}$, тогда $N = 10B + a_0$. Теперь поставим последнюю цифру a_0 на первое место, получим число $\overline{a_0a_5a_4a_3a_2a_1}$. Заметим, что

$$\overline{a_0a_5a_4a_3a_2a_1} = \overline{a_000000} + \overline{a_5a_4a_3a_2a_1} = 10^5 \cdot a_0 + B.$$

После вычитания полученного числа из исходного, получим

$$10B + a_0 - (10^5 \cdot a_0 + B) = 9B - 99999 \cdot a_0.$$

Данная запись показывает, что полученная разность делится на 9, таким образом, из чисел промежутка $[618222; 618252]$ могут подойти только числа, делящиеся на 9: 618228, 618237, 618246.

Осталось объяснить, почему каждое из этих чисел подходит.

Найдем хотя бы одно решение уравнения $9B - 99999 \cdot a_0 = 618228$, где B – произвольное пятизначное число, а a_0 – ненулевая цифра. Поделив обе части на 9, получим:

$$B - 11111 \cdot a_0 = 68692.$$

Взяв $a_0 = 1$, получим $B = 79803$ и исходное шестизначное число $N = 10B + a_0 = 798031$. Следовательно, 618228 – подходит.

Аналогичным образом, при $N = 798041, 798051$ в качестве разности мы получим два других числа: 618237, 618246, ч.т.д.

Ответ: 618228, 618237, 618246.

*
Пример 9 (ЕГЭ-2013, Уральский регион

а) Чему равно количество способов записать число 1292 в виде $a_0 \cdot 10^3 + a_1 \cdot 10^2 + a_2 \cdot 10 + a_3$, где числа a_i – целые, $0 \leq a_i \leq 99$, $i = 0,1,2,3$?

б) Существуют ли 10 различных чисел N, которые можно представить в виде $a_0 \cdot 10^3 + a_1 \cdot 10^2 + a_2 \cdot 10 + a_3$, где числа a_i – целые, $0 \le a_i \le 99$, $i = 0,1,2,3$ ровно 130 способами.

в) Сколько существует таких чисел N, которые можно представить в виде $a_0 \cdot 10^3 + a_1 \cdot 10^2 + a_2 \cdot 10 + a_3$, где числа a_i – целые, $0 \le a_i \le 99$, $i = 0,1,2,3$ ровно 130 способами.

Замечание. Насколько известно автору, в Уральском регионе эту задачу полностью не решил никто (даже призеры финала всероссийской олимпиады школьников). И это даже с учетом того, что автор видел условия ЕГЭ по математике 2013 года, включая прототип этой задачи, в свободном доступе в сети интернет за 3 дня до написания ЕГЭ. В других зонах (Центр, Сибирь, Дальний Восток) был значительно более легкий прототип задачи С6, с которым не возникло особых сложностей, а вот Уралу «повезло». Возможно, прорешивающим ЕГЭ прошлого года все же интересно, как все же должна решаться эта задача, поэтому удовлетворим их любопытство.

Решение.

Заметим, что число $a_0 \cdot 10^3 + a_1 \cdot 10^2 + a_2 \cdot 10$ делится на 10, поэтому число a_3 мы можем выбрать десятью способами – это будет любое из чисел от 0 до 99, оканчивающееся на 2. Поэтому, число $a_0 \cdot 10^3 + a_1 \cdot 10^2 + a_2 \cdot 10$ будет равняться числам, делящимся на 10, от 1200 до 1290. Написав для числа 1200, например, уравнение $a_0 \cdot 10^3 + a_1 \cdot 10^2 + a_2 \cdot 10 = 1200$ и, разделив на 10, получим, $a_0 \cdot 10^2 + a_1 \cdot 10^1 + a_2 = 120$. Фактически, мы пришли к задаче такого же типа, но на «уровень меньше» - уравнение теперь зависит от трёх переменных, а не четырёх. Такой способ задает начало перебора, который можно довести до конца и получить ответ 130. Однако пункт в) с помощью такого перебора решить уже проблематично.

Поэтому, приведем более простое решение этой задачи, основанное на следующем факте Разложение $a_0 \cdot 10^3 + a_1 \cdot 10^2 + a_2 \cdot 10 + a_3$ задавало бы число 1292 единственным образом, если бы a_0, a_1, a_2, a_3 были бы цифрами, то есть $0 \le a_i \le 9$, $i = 0,1,2,3$. Здесь же $0 \le a_i \le 99$, $i = 0,1,2,3$, поэтому разложение может быть неоднозначным.

А вот число $a_1 \cdot 10^2 + a_3$, $0 \le a_{1,} a_3 \le 99$, наоборот, уже однозначно задает любое число от 0 до 9999. Фактически, это равносильно заданию числа не в десятичной системе, а в системе с основанием 100, тогда a_1 и a_3 были бы просто «цифрами» у этого числа. Аналогично, и число $a_0 \cdot 10^2 + a_2$также задает однозначно любое число от 0 до 9999.

Поэтому, остается переформулировать задачу следующим образом.

Скольким количеством способов можно представить число 1292 в виде $A_0 \cdot 10 + A_1$, где $0 \leq A_0, A_1 \leq 9999$? Эта задача перебирается уже гораздо проще – у нас есть 130 способов взять число A_0 (от 0 до 129) и единственным образом подобрать к нему число A_1. В пункте а) ответ 130. Этот ответ никак не зависит от последней цифры числа 1292, у числе 1290, …, 1299 также будет ответ 130, поэтому в пункте б) ответ – существуют.

В пункте в) нужно найти все числа X, которые можно представить в виде $A_0 \cdot 10 + A_1$, где $0 \leq A_0, A_1 \leq 9999$, 130-ю способами. Для этого заметим, что совокупность числа вида $X - A_0 \cdot 10$ при разных A_0 представляют собой арифметическую прогрессию из целых чисел. Количество чисел в этой прогрессии – 10000, разность этой прогрессии – 10. И ровно 130 из этих чисел прогрессии должны быть в пределах от 0 до 9999 и давать подходящее по условию число A_1. Возможны два случая.

Первый – прогрессия пересекается с множеством чисел 0, …, 9999 по последним (самым большим) членам. Тогда эта прогрессия должна закончиться каким-то числом из множества 1290,1291,…,1299. Считая, что $A_0 = 0$ ($(X - A_0 \cdot 10)$ – самое большое число из прогрессии), получаем исходные числа равными вышеприведенным 1290,1291,…,1299.

Второй случай – прогрессия пересекается с множеством чисел 0, …, 9999 по первым (самым маленьким) членам. Тогда эта прогрессия должна начинаться каким-то числом из множества 8700, …, 8709. В этих число $A_0 = 9999$ и исходные числа, равные 108690,…, 108690 (в условии не сказано, что исходные числа обязаны быть четырёхзначными)

Итого, при 20 вариантах чисел существует 130 способов представить эти числа в виде, приведенном в условии задачи.

Ответ: а) 130 б) существуют в) 20.

§3. Деление целых чисел с остатком

3.1. Основные понятия и факты

Теорема о делении с остатком.

Всякое целое число m можно разделить с остатком на любое натуральное число n, т. е. однозначным образом представить в виде:

$$m = nq + r, 0 \le r < n,$$

где q – (целое число) *частное*, а r – остаток от деления m на n.

Алгоритм деления с остатком заключается в следующем. Если $0 \le m < n$, то следует принять $q = 0, r = m$, а если $m > n$, то из большего числа m следует вычитать меньшее n, пока не получится число, меньшее, чем n – остаток. В случае, если m– отрицательное, к нему надо, наоборот, прибавлять число n, пока не получится *неотрицательное* число, меньшее n – остаток.

Например, найдём остаток при делении числа 31 на число 7. Если вычесть четыре раза число 7 из числа 31, получим число $3 < 7$, таким образом, $31 = 4 \cdot 7 + 3$, остаток равен 3.

Теперь найдём остаток от деления числа -31 на число 7. Заметим, что домножив на (-1) предыдущее равенство, получим $-31 = (-4) \cdot 7 - 3$, но из этого не следует, что (-3) – остаток. Остаток должен быть неотрицательным. Таким образом, четырёх прибавлений числа 7 к числу (-31) недостаточно, нужно прибавить число 7 пятый раз и получить $-31 = (-5) \cdot 7 + 4,$ т. е. остаток равен 4.

Из теоремы о делении с остатком вытекает, что *среди любых подряд выписанных n чисел ровно одно кратно* n, остальные числа дают все остатки подряд от 1 до $n - 1$ (начиная, возможно, не с 1). Воспользовавшись этим, сформулируем следующие утверждения:

1. Произведение любых двух последовательных целых чисел делится на 2.

2. Произведение любых трёх последовательных целых чисел делится на 6.

3. Произведение любых четырёх последовательных целых чисел делится на 24.

Действительно, среди любых двух подряд идущих целых чисел одно чётное, значит, произведение тоже делится на 2.

Среди трёх подряд идущих чисел одно делится на 3. Также среди первых двух из трёх подряд идущих чисел одно делится на 2. Т. к. 2 и 3 взаимно простые, то произведение всех трёх чисел делится на 6.

Свойство 3 доказывается аналогично: среди подряд идущих 4-х чисел найдётся число, делящееся на 4, а так же ещё одно число, дающее остаток 2 при делении на 4, которое также будет чётным. Таким образом, произведение 4-х подряд идущих чисел делится на 4 × 2 = 8. Поскольку это произведение ещё делится на 3, а НОД(3,8) = 1, то произведение всех 4-х подряд идущих чисел делится на 24.

Пример 10. Докажите, что при любом нечётном *n* число $n^3 + 3n^2 - n - 3$ делится на 48.

Решение. Разложим данный многочлен: $n^3 + 3n^2 - n - 3 = (n - 3)(n^2 - 1) = (n - 3)(n - 1)(n + 1)$. Заметим, что n – нечётное, поэтому его можно представить в виде $n = 2k + 1$. Тогда $(n-3)(n-1)(n+1) = (2k-2)2k(2k+2) = 8(k-1)k(k+1)$. Произведение 3-х подряд идущих чисел делится на 6, поэтому всё произведение делится на 48.

Пример 11. Найдите все простые числа p, при которых числа $2p + 1$ и $4p + 1$ также являются простыми.

Решение. Идея решения заключается в том, что хотя бы одно из чисел $p,\ p+1,\ p+2$ должно делиться на 3, а следовательно, равняться трём (эти числа по условию простые).

Действительно, если p делится на 3, а p – простое число, то $p = 3$, числа $7 = 2 \cdot 3 + 1$ и $13 = 4 \cdot 3 + 1$ также простые.

Если $p + 1$ делится на 3, то $4(p + 1)$ также делится на 3, и число $4p + 1 = 4(p + 1) - 3$ также делится на 3. Это число по условию должно быть простым и потому может быть равным только трём, но $4p + 1 \neq 3$.

Если $p + 2$ делится на 3, то $2(p + 2)$ также делится на 3, и простое число $2p + 1 = 2(p + 2) - 3$ также делится на 3. Но это число простое, и если $2p + 1 = 3,$ то $p = 1$ не является простым числом, противоречие.

Ответ: $p = 3$.

3.2. Признаки делимости

Вспомним некоторые из признаков делимости и выведем дальнейшие. Пусть натуральное число имеет десятичную запись:

$$\overline{a_n a_{n-1} \dots a_2 a_1 a_0} = 10^n a_n + 10^{n-1} a_{n-1} + \cdots + 10^2 a_2 + 10a_1 + a_0,$$

Сформулируем несколько *признаков делимости,* известных вам из школьного курса, разделив их на три группы.

1. Признаки делимости *по нескольким последним цифрам*:

Если …	***то а делится на …***
a_0 *делится на* 2 *или на* 5	2 *или* 5 *соответственно*
$\overline{a_1 a_0}$ *делится на* 4 *или на* 25	4 *или* 25 *соответственно*
$\overline{a_2 a_1 a_0}$ *делится на* 8	8
a_0 *равно* 0	10
$\overline{a_{n-1} a_{n-2} \dots a_1 a_0}$ *равно* 0	10^n

Доказательство всех этих признаков содержат одну и ту же идею, продемонстрируем её на примере признака делимости на 4.

Заметим, что

$$\overline{a_n a_{n-1} \dots a_2 a_1 a_0} = \overline{a_n a_{n-1} \dots a_2 00} + \overline{a_1 a_0} =$$
$$= 100 \times \overline{a_n a_{n-1} \dots a_2} + \overline{a_1 a_0}.$$

Но, число 100 делится на 4, поэтому $100 \times \overline{a_n a_{n-1} \dots a_2}$ также делится на 4, поэтому делимость исходного числа на 4 зависит только от того, делится ли $\overline{a_1 a_0}$ на 4 или нет.

Замечание. Все признаки сформулированные, выше, являются также и ***признаками равноостаточности:*** остаток от деления на соответствующий делитель исходного числа и выражения, записанного в левой части таблицы совпадает. *Этому свойству будут удовлетворять и все признаки, которые будут записаны ниже.*

2. Признаки делимости *по сумме цифр.*

Если …	***то а делится на …***
сумма цифр делится на 3 *или* 9	3 *или* 9 *соответственно*
знакочередующаяся сумма делится на 11	11

Докажем признак делимости на 9.

$$\overline{a_n a_{n-1} \dots a_2 a_1 a_0} = 10^n a_n + 10^{n-1} a_{n-1} + \dots + 10^2 a_2 + 10 a_1 + a_0 =$$
$$\left(\underbrace{99 \dots 9}_{n} a_n + \underbrace{99 \dots 9}_{n-1} a_{n-1} + \dots + 99 a_2 + 9 a_1\right) +$$
$$+ (a_n + a_{n-1} + \dots + a_2 + + a_1 + a_0) =$$
$$= 9 \times \left(\underbrace{11 \dots 1}_{n} a_n + \underbrace{11 \dots 1}_{n-1} a_{n-1} + \dots + 11 a_2 + 1 a_1\right) +$$
$$+ (a_n + a_{n-1} + \dots + a_2 + a_1 + a_0).$$

Делимость последнего выражения на 9 совпадает с делимостью суммы цифр исходного числа на 9.

Теперь, докажем признак делимости на 11.

Заметим, что числа 11, 1001, 100001 (и вообще, все нечётные степени десятки, увеличенные на 1), делятся на число 11. Это легко проверить. Действительно, $1001 = 990 + 11$, $100001 = 99990 + 11$ и т. д., откуда делимость на 11 становится очевидной. Более строго это следует из формулы сокращённого умножения, которая в нашем случае может быть записана в виде:

$$(10 + 1)^{2k+1} = (10 + 1)\left(10^{2k} - 10^{2k-1} + \dots + 10^2 - 10 + 1\right).$$

Числа, состоящие из чётного числа девяток (99, 9999 – чётные степени десятки, уменьшенные на 1), делятся на число 99 и, следовательно, на число 11.

Тогда наше число a может быть переписано в виде:

$$a = a_0 + (11 - 1) a_1 + (99 + 1) a_2 + (1001 - 1) a_3 + \dots =$$

$$= (a_0 - a_1 + a_2 - a_3 + \cdots) + \left(\underline{11}a_1 + \underline{99}a_2 + \underline{1001}a_3 + \cdots\right).$$

Все подчёркнутые числа кратны 11, следовательно, остаток от деления на число 11 равен остатку знакочередующейся суммы цифр.

Пример 12. При каких натуральных n число $4^n + 1$ делится на 5?

Решение. Посмотрим на последнюю цифру числа 4^n.

n	1	2	3	4	5
4^n	4	16	64	256	1024

Несложно заметить, что при чётных степенях она будет равняться шести, при нечётных – четырём. Эта закономерность будет продолжаться и дальше: умножая на 4 число, оканчивающееся на 6, мы получим число с последней цифрой 4 и, наоборот, умножая на 4 число с последней цифрой 4, мы получим число, оканчивающееся на 6.

Если прибавить единицу, мы получим, что последняя цифра полученного числа равняется 5 при нечётных степенях, и равняется 7 при чётных. По признаку делимости на 5 последняя цифра числа, делящегося на 5, должна быть либо 0, либо 5, поэтому $4^n + 1$ делится на 5 только при нечётных n.

Ответ: $4^n + 1$ делится на 5 при нечётных n и не делится – при чётных.

*В последней группе признаков делимости рассматриваются суммы двузначных или трёхзначных граней – двузначных или трёхзначных чисел из цифр данного числа, справа налево. Так, в числе 12345 есть три двузначные грани: 1 | 23 | 45.

3. Признаки делимости *по сумме граней.*

Если …	***то а делится на …***
сумма двузначных граней делится на 11	11
сумма трёхзначных граней делится на 37	37
знакочередующаяся сумма трёхзначных граней делится на 7, 11, 13	7, 11 13 *соответственно*

Докажем, например, второй признак делимости на 11.

$$\overline{a_n a_{n-1} \dots a_2 a_1 a_0} = \overline{a_1 a_0} + 100\overline{a_3 a_2} + 10000\overline{a_5 a_4} + \cdots =$$
$$= (\overline{a_1 a_0} + \overline{a_3 a_2} + \overline{a_5 a_4} + \cdots) + (99\overline{a_3 a_2} + 9999\overline{a_5 a_4} + \cdots).$$

Т. к. 99 делится на 11, то число в правой скобке делится на 11, следовательно, делимость исходного числа на 11 зависит от суммы двузначных граней, написанной в первой скобке.

Хотя доказательство оставшихся двух признаков является аналогичным доказанному признаку и мы приводить его не будем, отметим разложение числа 1001 на простые множители, которое позволило сформулировать признаки делимости на 7, 11 и 13:

$$1001 = 7 \times 11 \times 13.$$

Пример 13. Делится ли на 7 число 1234567890?

Решение. Воспользуемся признаком делимости на 7 и посчитаем знакочередующуюся сумму трёхзначных граней: 890 – 567 + 234 – – 1 = 556. Число 556 на 7 не делится, значит, исходное число на 7 также не делится.

Ответ: не делится. *

3.3. Вычисление НОД с помощью алгоритма Евклида

Чтобы вычислить НОД двух чисел, не обязательно знать разложение этих чисел на простые множители. Существует иной способ, основанный на делении с остатком. Он известен как ***алгоритм Евклида***.

Сформулируем свойство НОД двух чисел, которое используется в алгоритме Евклида. Пусть $a > b$, тогда

$$\text{НОД}(a, b) = \text{НОД}(a - b, b).$$

Это легко доказывается при помощи свойства 2 делимости целых чисел. Докажем, что общие делители чисел a, b и чисел $a - b, b$ совпадают. Действительно, пусть a, b делятся на k, тогда $a - b$, также делится на k. Обратно, пусть $a - b, b$ делятся на k. Тогда $a = (a - b) + b$ также на него делится. Если все общие делители совпадают, то наибольший из них (НОД) также должен совпадать.

Теперь перейдём к формулировке *алгоритма Евклида*. Пусть $a > b$. Разделим с остатком число a на число b: $a = bq + r,\ 0 \leq r < b$. Тогда

$$\text{НОД}(a, b) = \text{НОД}(r, b) = \text{НОД}(b, r).$$

Это свойство получается многократным применением свойства НОД(a, b) = НОД($a - b, b$). Теперь заменим число a на число b, b – на число r и проделаем тоже самое с числами b и r и т. д. Эти операции закончатся, когда одно число поделится на другое нацело, делитель и будет являться НОД чисел a и b.

Пример 14. С помощью алгоритма Евклида найдите НОД чисел 1848 и 627.

Решение. Начнём операцию деления с остатком:

$1848 = 627 \times 2 + 594$, поэтому НОД(1848,627) = НОД(627,594),

$627 = 594 \times 1 + 33$, поэтому НОД(627,594) =НОД(594,33),

$594 = 33 \times 18$, т. е. число 594 разделилось на 33 нацело. Это означает, что за 3 шага алгоритм Евклида выдал ответ 33.

Ответ: НОД$(1848{,}627) = 33$.

Пример 15. Докажите, что при целых значениях x числа $2x^2 + 4$ и $2x - 1$ не могут одновременно делиться ни на какие простые числа, отличные от 3.

Решение. Для доказательства применим алгоритм Евклида. Найдём, какие значения может принимать НОД$(2x^2 + 4,\ 2x - 1)$. Для этого, воспользовавшись несколько раз свойством в начале параграфа, получим: НОД$(2x^2 + 4,\ 2x - 1)$ =НОД$(x + 4,\ 2x - 1)$. Это следует из того, что $2x^2 + 4 = (x + 4) + x(2x - 1)$. $(x + 4,\ 2x - 1)$.

Вычтя из $2x - 1$ дважды число $x + 4$, получим: НОД$(2x - 1,\ x +$ $+4=$ НОД$9,\ x+4.$ Число 9 не зависит от $x,$ это значит, что НОД$9,\ x+4,$ который равняется НОД исходных выражений, делит число 9. Таким образом, НОД$(2x^2 + 4,\ 2x - 1)$ может принимать значения 1, 3, 9, из чего и следует утверждение задачи.

Алгоритму Евклида уже более 2 тыс. лет. Он сформулирован в «Началах» Евклида, где из него выводятся свойства простых чисел, наименьшего общего кратного и т. д. Алгоритм имеет много практических применений. Ещё древние пифагорейцы знали его как способ нахождения наибольшей общей меры двух соизмеримых отрезков. К середине XIV в. алгоритм Евклида был распространён на многочлены от одного переменного, а в дальнейшем этот алгоритм был определён и для ряда других алгебраических объектов.

§4. Решение уравнений в целых числах

4.1. Линейное диофантово уравнение с двумя неизвестными

В этом разделе рассматривается линейное уравнение

$$ax + by = c,$$

где a, b, c – целые числа, причем $ab \neq 0$ (иначе это уравнение с не более одной неизвестной).

Уравнения с целыми числами с двумя (и более) неизвестными наряду с большим количеством других интересных задач рассматривал в своей книге «Арифметика» греческий математик Диофант Александрийский (III в.). Такие уравнения были впоследствии названы его именем.

Пример 16. Докажите, что монетами в 2 и 5 рублей можно заплатить любую натуральную сумму рублей, кроме 1 и 3.

Решение. Пусть сумма, которую нужно составить, равняется n рублей, и мы заплатим её x монетами по 2 рубля и y монетами по 5 рублей.

Отсюда получим уравнение $2x + 5y = n$. Выразим x через y: $x = \frac{n-5y}{2}$.

Наша задача – найти хотя бы одно решение этого уравнения в целых неотрицательных числах. Если n делится на 2, то в качестве такого решения можно взять $y = 0$, $x = n/2$. Если же n не делится на 2, то можно взять $y = 1$, $x = \frac{n-5}{2}$. Здесь x не будет являться отрицательным, если $n \geq 5$. Таким образом, любую натуральную сумму рублей, кроме 1 и 3 можно заплатить монетами в 2 и 5 рублей.

Замечание. Если же в этой задаче разрешить давать сдачу (также только монетами 2 и 5 рублей), то тогда можно будет с учётом сдачи заплатить любую сумму рублей.

Перейдём к решению уравнения $ax + by = c$.

Теорема. **Уравнение $\boldsymbol{ax + by = c}$ имеет бесконечное множество целочисленных решений, если $\boldsymbol{c}$ делится на НОД$(\boldsymbol{a, b})$ и не имеет целочисленных решений в противном случае.**

Условие «c делится на НОД(a, b)», частности, всегда выполнено, когда числа a и b взаимно просты.

Диофантово уравнение $ax + by = c$ можно решать по следующему алгоритму:

1. Разделим обе части уравнения $ax + by = c$ на НОД(a, b). Числа a и b, поделённые на свой НОД, станут взаимно простыми. Если число c, разделённое нацело на НОД(a, b), не является целым, то уравнение решений не имеет (слева стоит целое число, справа – нецелое). Таким образом, мы пришли к равносильному уравнению $\bar{a}x + \bar{b}\,y = \bar{c}$, где НОД$(\bar{a}, \bar{b}) = 1$.

2. Итак, пусть теперь есть уравнение $ax + by = c$, где числа a и b являются взаимно простыми. Найдём какое-то одно (так называемое «частное») решение этого уравнения – (x_0, y_0). Это можно сделать путём подбора или с помощью алгоритма Евклида (см. конец этого раздела).

3. Выпишем ответы: $\begin{cases} x = x_0 - bt \\ y = y_0 + at \end{cases}, \quad t \in \mathbb{Z}.$

Почему все ответы имеют такой вид?

Пусть (x_0, y_0) – решение уравнения $ax + by = c$. Рассмотрим выражение $a(x - x_0) + b(y - y_0)$. Оно равняется нулю: $a(x - x_0) + {}$ $+ b(y - y_0) = ax + by - (ax_0 + by_0) = c - c = 0$.

Таким образом, числа $x - x_0$ и $y - y_0$ являются решениями уравнения $aX + bY = 0$. Перепишем это уравнение в виде $aX = -bY$. Так как числа a и b – взаимно просты, число Y должно делиться на число a, т. е. $Y = at$ при каком-то целом t. Подставим Y в уравнение $aX = -bY$, получим $aX = -bat$, что в свою очередь после сокращения на a преобразуется к виду $X = -bt$. Итак, $\begin{cases} x - x_0 = -bt, \\ y - y_0 = at, \end{cases}$

откуда и получаем выписанные в п. 3 ответы.

Пример 17. Решите уравнение $10x + 4y = 100$.

Решение. Разделим обе части уравнения на НОД(10,4) = 2, получив уравнение $5x + 2y = 50$. Подбором получаем частное решение $x_0 = 10,\ y_0 = 0$.

Затем выпишем все решения этого уравнения: $\begin{cases} x = 10 - 2t \\ y = 5t \end{cases}$, $t \in \mathbb{Z}$.

Ответ: $\begin{cases} x = 10 - 2t \\ y = 5t \end{cases}$, $t \in \mathbb{Z}$.

*Опишем процесс нахождения «частного» решения с помощью алгоритма Евклида на примере диофантова уравнения $7x + 18y = 2$.

Пример 18. Найдите частное решение уравнения $7x + 18y = 2$.

Решение. Для начала найдём частное решение уравнения $7x + 18y = 1$, затем, домножим полученное решение на 2, получим частное решение уравнения $7x + 18y = 2$.

Найдём НОД(18,7) с помощью алгоритма Евклида. 18 = 7 × 2 + 4, поэтому НОД(18,7) = НОД(7,4). Будем записывать каждое новое число, к которому мы приходим, выполняя алгоритм Евклида, в виде $7x + 18y$. Так, 4 = 18 – 7 × 2.

Затем НОД(7,4) = НОД(4,3), где 3 = 7 – 4 = 7– (18 –7×2) = 7×3 – 18.

Наконец, НОД(4,3) = НОД(3,1) = 1, причём 1 = 4 – 3 = (18 – 7×2) – – (7×3 –18) = 18×2 – 7×5.

Вот, мы получили частное решение уравнения $7x + 18y = 1$: $x = -5, y = 2$.

Отсюда частное решение уравнения $7x + 18y = 2$ имеет вид $x_0 = -10,\ y_0 = 4$.

Решая задачу другими способами, можно найти и другие частные решения. Например, $x_0 = 8,\ y_0 = -3$.

Ответ: $x = -10, y = 4$. *

4.2. Примеры решения нелинейных уравнений

Пример 19. *(ЕГЭ, тренировочный вариант)* Группу школьников нужно перевезти из летнего лагеря одним из двух способов: либо двумя автобусами типа А за несколько рейсов, либо тремя автобусами типа В за несколько рейсов, причём в этом случае число рейсов каждого автобуса типа В будет на один меньше, чем рейсов каждого автобуса типа

А. В каждом из случаев автобусы заполняются полностью. Какое максимальное количество школьников можно перевезти при указанных условиях, если в автобус типа В входит на 7 человек меньше, чем в автобус типа А.

Решение. Пусть в автобус типа В входит x человек (тогда в автобус типа А входит $x+7$ человек), и автобусы типа В должны совершить y рейсов (тогда автобусы типа А должны совершить $y+1$ рейс). По условию задачи составим выражение для количества детей, перевезённых обоими способами:

$$2(x+7)(y+1) = 3xy.$$

Выразим переменную x этого выражения через y.

$$14y + 2x + 14 - xy = 0; \quad x = \frac{14y+14}{y-2}.$$

Выделим целую часть числа: $\frac{14y+14}{y-2}$; $x = \frac{14y+14}{y-2} = 14 + \frac{42}{y-2}$.

Напомним, число x должно быть целым, отсюда получаем, что число $(y-2)$ должно быть делителем числа 42.

Переберём все делители числа 42 и выясним, какое максимальное количество детей $(3xy)$ можно увезти:

$y-2$	1	2	3	6	7	14	21	42
y	3	4	5	8	9	16	23	44
x	56	35	28	21	20	17	16	15
$3xy$	504	420	420	504	540	816	1104	1980

Максимальное количество школьников, которое можно перевезти согласно условиям задачи, равно 1980.

Ответ: 1980.

Пример 20. Решите в целых числах уравнение $xy = 5(x+y)$.

Решение. Перепишем уравнение в виде: $xy - 5x - 5y = 0$;

$x(y-5) - 5(y-5) - 25 = 0$; $(x-5)(y-5) = 25$.

Заметим, что 25 можно разложить на множители (в том числе отрицательные) только следующими способами: $25 = 1 \times 25 = 5 \times 5 = (-1) \times (-25) = (-5) \times (-5)$.

Из каждого из разложений получаем решения.

Ответ: $(x, y) = (6,30); (30,6); (10; 10); (4, -20); (-20,4); (0,0)$.

Пример 21. Решите в целых числах уравнение

$$x^2 = 2y^2 + xy + 7.$$

Решение. Перепишем это уравнение в виде: $(x+y)(x-2y) = 7$.

Это разложение можно получить следующим образом: запишем выражение $x^2 - xy - 2y^2 = 0$ и вынесем y^2 за скобки: $y^2\left[\left(\frac{x}{y}\right)^2 - \frac{x}{y} - 2\right]$.

Далее, решив квадратное уравнение $\left(\frac{x}{y}\right)^2 - \frac{x}{y} - 2 = 0$ (корни $\frac{x}{y} = -1$, $\frac{x}{y} = 2$, разложим его на множители. $\left(\frac{x}{y}+1\right)\left(\frac{x}{y}-2\right)$. Отсюда, после домножения на y^2, получается написанное выше разложение:

$$(x+y)(x-2y).$$

Т. к. $(x+y)$ и $(x-2y)$ – целые числа, то нужно посмотреть на разложение числа 7 на два целых множителя. Возможные разложения выпишем в таблицу:

$x+y=$	7	1	-7	-1
$x-2y=$	1	7	-1	-7

Получаются 4 системы линейных уравнений. Решим одну из них (первую):

$$\begin{cases} x+y=7, \\ x-2y=1. \end{cases}$$

Получим: $x=5, y=2$.

Остальные системы выписываются аналогично, и все полученные решения будут являться целыми.

Ответ: $(x,y) = (5,2); (-5,-2); (3;-2); (-3;2)$.

В обоих примерах мы раскладывали многочлен на множители и использовали свойства делимости.

Пример 22. Решите в целых числах уравнение $x^3 - xy - 7x + 2y + {}$ $+23 = 0$.

Решение. В это уравнение переменная y входит в первой степени, выразим её через x: $x^3 + y(2-x) - 7x + 23 = 0$, $y = \frac{x^3 - 7x + 23}{x-2}$.

Сделаем замену: $t = x-2$. Тогда $x = t+2$; $x^3 = t^3 + 6t^3 + 12t + 8$ и, следовательно,

$$y = \frac{t^3 + 6t^3 + 12t + 8 - 7t - 14 + 23}{t} = t^2 + 6t + 5 + \frac{17}{t}.$$

По условию y и t – целые, поэтому 17 должно делиться на t. Возможны варианты:

t	1	-1	17	-17
x	3	1	19	-15
y	29	17	397	191

Ответ: $(x, y) = (3,29); (1,17); (19,397); (-15; 191)$.

Пример 23. Найдите все целые x, при которых $2^n + 1 = x^2$, где n – натуральное число.

Решение. Будем считать x неотрицательным (затем добавим число "$-x$" в ответ)

Перепишем это уравнение в виде $2^n = x^2 - 1 = (x-1)(x+1)$.

Заметим, что неотрицательные делители числа 2^n также обязаны являться степенями двойки, поэтому $(x-1) = 2^i$, $(x+1) = 2^j$. Числа $(x-1)$ и $(x+1)$ – делители числа 2^n - не равны единице, поэтому оба этих числа являются натуральными степенями двойки. С другой стороны, среди двух последовательных чётных чисел одно делится на 4, а второе на 4 не делится. Поскольку второе число на 4 не делится и при этом оно не должно содержать отличных от 2 простых делителей, то это число равно 2.

Таким образом, нужно рассмотреть 2 случая:

а. $(x+1) = 2, x = 1$ – не подходит.

б. $(x-1) = 2, x = 3$ – подходит ($n = 3$).

Ответ: $x = \pm 3, n = 3$.

Пример 24. Решите в натуральных числах уравнение

$$1 + x + x^2 + x^3 = 2^y.$$

Решение. Разложив левую часть, получим $(1+x)(1+x^2) = 2^y$. Т. к. числа x и x^2 – натуральные, $1 + x \geq 2; 1 + x^2 \geq 2$, значит, оба числа – $(1+x)$ и $(1+x^2)$ являются натуральными степенями двойки. Пусть $1 + x = 2^t$. Выразив из этого уравнения x, получим, $1 + x^2 = 2^{2t} - 2 \cdot 2^t + 2$. Это число также должно являться степенью двойки.

Если $t = 1$, то $(x, y) = (1,2)$ – решения нашего уравнения.

Если $t = 2$, то $1 + x^2 = 10$, что не является степенью двойки; решений в данном случае нет.

Если $t \geq 3$, то $2 \cdot 2^t - 2 > 0$ и $2^{2t} - 2 \cdot 2^t + 2 < 2^{2t}$. Докажем, что $2^{2t} - 2 \cdot 2^t + 2 > 2^{2t-1}$. Это неравенство можно переписать в виде $2^{2t-1} = 2^{2t} - 2^{2t-1} > 2 \cdot 2^t - 2$; $2^{2t-2} > 2^t - 1$.

Последнее неравенство является верным, т. к. при $t \geq 3$ верно $2t - 2 > t$, что приведёт к неравенству $2^{2t-2} - 2^t > 0 > -1$.

Таким образом, мы получили, что число $1 + x^2 = 2^{2t} - 2 \cdot 2^t + 2$ заключено строго между двумя соседними степенями двойки, $2^{2t-1} <$

$2^{2t} - 2 \cdot 2^t + 2 < 2^{2t}$, а, значит, само степенью двойки не является. Противоречие, решений при $t \geq 3$ нет.

Ответ: $(x, y) = (1,2)$.

*§5. Сравнения

Пусть задано натуральное число n, которое мы в дальнейшем будем называть *модулем.*

Будем говорить, что **числа a и b сравнимы по модулю n, если $a - b$ делится на n**. Это утверждение обозначают как

$$a \equiv b \pmod{n}.$$

Если число $a - b$ не делится на n, то говорят, что a не сравнимо с b по модулю n, и обозначают как $a \not\equiv b \pmod{n}$.

По теореме о делении с остатком числа a и b можно представить в виде:

$$a = k_1 n + r_1,\ 0 \leq r_1 < n;\quad b = k_2 n + r_2,\ 0 \leq r_2 < n,$$

где r_1 и r_2 – остатки, возникающие при делении чисел a и b на число n. Заметим, что $r_1 = a - k_1 n$; $r_2 = b - k_2 n$, откуда $r_1 - r_2 = (a - b) + +n(k_2 - k_1)$. Отсюда, если $a - b$ делится на n, то $r_1 - r_2$ также делится на n. Т. к. $0 \leq r_1 < n$, $0 \leq r_2 < n$, то $-n < r_1 - r_2 < n$. Поэтому $r_1 - r_2$ делится на n только в одном случае: $r_1 - r_2 = 0$, $r_1 = r_2$. Очевидно, верно и обратное: если $r_1 = r_2$, то $a - b$ делится на n.

Поэтому **числа a и b сравнимы по модулю n тогда и только тогда, когда они дают одинаковые остатки при делении на n.**

Рассмотрим множество чисел, которые дают остаток r при делении на n (это множество является подмножеством целых чисел). Из утверждения выше следует, что любые два числа из данного множества будут сравнимы между собой по модулю n. Всего разных остатков при делении на n имеется n штук (от 0 до $n - 1$). Таким образом, множество целых чисел можно разбить на n множеств, не содержащих общих элементов, каждое из которых характеризуется остатком от деления чисел множества на n.

Например, при $n = 3$ будет три множества: множество чисел, делящихся на 3 (имеет вид $3k, k \in \mathbb{Z}$); множество чисел, дающих остаток 1 при делении на 3 ($3k + 1, k \in \mathbb{Z}$), и множество чисел, дающих остаток 2 при делении на 3 ($3k + 2, k \in \mathbb{Z}$).

Такие множества называются *классами вычетов.* Таким образом множество целых чисел разделено на n классов вычетов по модулю n.

Из всего вышесказанного следует, что **числа a и b сравнимы по модулю n тогда и только тогда, когда они принадлежат одному классу вычетов при делении на n.**

Основные свойства сравнений.

Свойство 1. (Сложение и вычитание сравнений)

Если $a \equiv b \pmod n$ и $c \equiv d \pmod n$, то $a \pm c \equiv (b \pm d) \pmod n$.

Следствие 1.1. К обеим частям сравнения можно прибавить одно и то же число: *если* $a \equiv b \pmod n$, то $a+c \equiv (b + c) \pmod n$.

Свойство 2. (Умножение сравнений).

Если $a \equiv b \pmod n$ и $c \equiv d \pmod n$, то $ac \equiv bd \pmod n$.

Следствие 2.1. Обе части сравнения можно умножать на одно и то же число: *если* $a \equiv b \pmod n$, то $ac \equiv bc \pmod n$.

Следствие 2.2. Обе части сравнения можно возводить в одну и ту же степень: *если* $a \equiv b \pmod n$, то $a^c \equiv b^c \pmod n$.

Пример 25. Доказать, что при любом натуральном n число $6^{2n} + 19^n - 2^{n+1}$ делится на 17.

Решение. Докажем, что $6^{2n} + 19^n - 2^{n+1} \equiv 0 \pmod{17}$.

Согласно свойству 1 сравнений, каждое число в сумме можно заменить на число, дающее такой же остаток при делении на 17. Заметим, $6^{2n} = 36^n$. Т. к. $36 \equiv 2 \pmod{17}$, то, согласно следствию 2.2, $36^n \equiv 2^n \pmod{17}$.

Аналогично, $19^n \equiv 2^n \pmod{17}$. Заменим числа 6^{2n} и 19^n на сравнимые им. Тогда потребуется доказать, что $2^n + 2^n - 2^{n+1} \equiv 0 \pmod{17}$, но это очевидно, т. к. в левой части сравнения при вычислении получается число 0.

Таким образом, $6^{2n} + 19^n - 2^{n+1} \equiv 0 \pmod{17}$, т. е. $6^{2n} + 19^n - 2^{n+1}$ делится на 17.

Приведём другой способ решения примера, который не использует свойства сравнений, но использует метод математической индукции, согласно которому, *если доказываемое утверждение верно при начальном* n_0, (обычно $n_0 = 1$) («основание индукции») *и из предположения, что доказываемое утверждение верно при* $n = k$ («предположение индукции») *следует его справедливость для* $n = k + 1$ («шаг индукции»), *то утверждение верно при всех* $n \geq n_0$.

Стоит отметить, что обе части (основание и шаг индукции) одинаково важны при доказательстве утверждений.

Вернёмся к примеру и проверим основание индукции при $n = 1$. Действительно: $6^2 + 19 - 2^2 = 51 \vdots 17$.

Пусть при $n = k$ выражение $A_k = 6^{2k} + 19^k - 2^{k+1}$ делится на 17 (предположение индукции). При $n = k + 1$, получим:

$$A_{k+1} = 6^{2(k+1)} + 19^{k+1} - 2^{(k+1)+1} = 36 \cdot 6^{2k} + 19 \cdot 19^k + 2 \cdot 2^{k+1}$$
$$= 36 \cdot \left(6^{2k} + 19^k + 2^{k+1}\right) - 17 \cdot 19^k - 34 \cdot 2^{k+1} =$$
$$= 36A_k - 17 \cdot 19^k - 34 \cdot 2^{k+1}.$$

Т. к. по предположению индукции $A_k \vdots 17$, то $A_{k+1} = 36A_k - -17 \cdot 19^k - 34 \cdot 2^{k+1}$ также делится на 17. Таким образом, шаг индукции доказан и, согласно методу математической индукции, исходное утверждение верно при всех $n \geq 1$.

Пример 26. Решите в целых числах уравнение $x^2 + y^2 = 151515$.

Решение. В данной задаче требуется применить сравнения по модулю 4. Остаток от деления числа x^2 на 4 зависит от остатка от деления числа x на тот же модуль. Выпишем все возможные остатки при делении числа x в таблицу, туда же запишем остатки от числа x^2.

остаток от x	0	1	2	3
остаток от x^2	0	1	0	1

Проверим, например, остаток 3. Действительно, $3^2 = 9 \equiv 1 (\mathrm{mod}\ 4)$.

Таким образом, по модулю 4 квадраты чисел могут давать только остатки 0 и 1, поэтому сумма двух квадратов может давать остатки 0, 1, 2 и не может давать остатка 3. Но, $151515 \equiv 3\ (\mathrm{mod}\ 4)$. Поэтому решений в целых числах у исходного уравнения нет.

Ответ: нет решений.

Пример 27. Существует ли натуральное число n такое, что $2012^{2012} + 2014^{2014} = n^2$?

Решение. В отличие от предыдущей задачи, если использовать сравнения по модулю 4, противоречия не получится. Действительно, оба числа 2012^{2012} и 2014^{2014} делятся на 4, т. е. n^2 должен давать остаток 0 при делении на 4, и такое возможно. Однако отсутствие противоречия при рассмотрении модуля 4 не гарантирует существования такого n. Модуль, по которому возникает противоречие, обычно ищут методом перебора среди возможных модулей.

Так, в этом примере возникает противоречие по другому модулю: $n = 3$. Заметим, $2012 \equiv 2 \equiv -1\ (\mathrm{mod}\ 3)$; $2014 \equiv 1\ (\mathrm{mod}\ 3)$. Воспользоваться зовавшись следствием 2.2 (возведение сравнения в степень), а затем свойством 1 (сложение сравнений), получим, $2012^{2012} + 2014^{2014} \equiv$ $\equiv (-1)^{2012} + 1^{2014} \equiv 2 \pmod 3$. Таким образом, квадрат натурального числа должен давать остаток 2 при делении на 3.

Однако квадраты натуральных чисел также могут давать только остатки 0 и 1 при делении на 3: ($0^2 \equiv 0 (\mathrm{mod}\, 3)$; $1^2 \equiv 1 (\mathrm{mod}\, 3)$; $2^2 \equiv$ $\equiv 1 \pmod 3$).

Следовательно, такого натурального n не существует.

Пример 28. Найдите остаток от деления $(36 \cdot 35)^{50}$ на 17.

Решение. Следствие 2.2 свойств сравнений (возведение сравнения в степень) позволяет основание степени $36 \cdot 35$ заменить на сравнимое с этим основанием по модулю 17 число. Это число мы найдём, воспользовавшись свойством 2 сравнений (умножение сравнений), заменив числа 36 и 35 на их остатки по модулю 17, т. е. на числа 2 и 1.

Записывая формулами вышесказанное: $36 \equiv 2 \pmod{17}$;

$35 \equiv 1 \pmod{17}$, получим $36 \cdot 35 \equiv 2 \cdot 1 \equiv 2 \pmod{17}$. Затем по следствию 2.2 $(36 \cdot 35)^{50} \equiv 2^{50} \pmod{17}$. Итак, нужно найти остаток от деления 2^{50} на 17.

Будем возводить число 2 последовательно в натуральные степени (1, 2, 3, 4, …) и посмотрим на остатки от деления получившихся чисел на 17. Всего теоретически возможно 16 разных остатков от деления числа 2^n на 17 (все, кроме 0). Таким образом остатки когда-то должны повториться. Выпишем в таблицу несколько первых степеней, найдём их остатки по модулю 17 и определим, когда остатки повторятся.

n	1	2	3	4	5	6	7	8	9	10
2^n	2	4	8	16	32	64	128	256	512	1024
остаток	2	4	8	16	15	13	9	1	2	4

Замечание. При выписывании таблицы остатков не обязательно вычислять все степени двойки, для вычисления остатка следующей степени достаточно знать остаток от предыдущей степени. Например, найдём остаток от 2^6 по модулю 17. Мы уже знаем, что $2^5 \equiv 15 \pmod{17}$. Тогда $2^6 = 2 \cdot 2^5$ и, по свойству 2 сравнений, получим $2 \cdot 2^5 \equiv 2 \cdot 15 \equiv$ $\equiv 30 \equiv 13 \pmod{17}$.

Итак, мы выписали первые 10 степеней двойки и нашли повторение: $2^9 \equiv 2^1 \equiv 2 \pmod{17}$. Т. к. из замечания выше следует, что остаток следующей степени зависит только от остатка текущей степени, далее остатки будут повторяться:

$$2^{10} \equiv 2^2 \equiv 4 \pmod{17};\ \ 2^{11} \equiv 2^3 \equiv 8 \pmod{17};$$
$$2^{12} \equiv 2^4 \equiv 16 \pmod{17}\ \text{ и т. д.}$$

Таким образом, эти остатки будут представлять собой периодическую последовательность с периодом $(9 - 1) = 8$.

Найдём теперь остаток от 2^{50}. Для этого найдём остаток от числа 50 по модулю периода последовательности – числа 8. Получим $50 \equiv \equiv 2 \pmod{8}$, поэтому $2^{50} \equiv 2^2 \equiv 4 \pmod{17}$.

Ответ: 4.

Приведём без доказательства теорему, полезную при решении задач на делимость степеней. Она принадлежит Пьеру Ферма, но, в отличие от Великой теоремы Ферма, легко доказывается и 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.**

На языке сравнений, если $a \not\equiv 0 \pmod{p}$, то $a^{p-1} \equiv 1 \pmod{p}$.

Малая теорема Ферма была бы полезна при решении предыдущего примера: так согласно теореме, $2^{16} \equiv 1 \pmod{17}$, поэтому $2^{50} = 2^{48} \cdot 2^2 = (2^{16})^3 \cdot 2^2 \equiv (1)^3 \cdot 2^2 \pmod{17} \equiv 4 (\mathrm{mod} 17)$, откуда сразу следует ответ 4. *

Контрольные вопросы

(*В контрольных вопросах числа* a, b *– целые,* n, m *– натуральные*)

1(2). Пусть ab делится на n. Верно ли, что a или b делится на n? (Сравните со свойством 4 делимости.)

2(2). Пусть a делится на m и n. Верно ли, что a делится на mn? (сравните со свойством 5 делимости).

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

5(2). Допишите последнюю цифру n числа $7654321n$ так, чтобы полученное число делилось на: 3, 9, 4, 8, 25, 11.

6(2). Найдите НОД(180,138) с помощью алгоритма Евклида.

7(2). Решите диофантово уравнение $15a - 9b = 12$.

Задачи

1(3). Докажите, что число $n^{4m} + n^{2m} + 1$ является составным при любых натуральных $n, m, n > 2$.

2(3). Докажите, что при всех целых n число $n^3 - 3n^2 - 4n + 2014$ не делится на 6.

3(3). Последние две цифры восьмизначного числа переставили на первые места в том же порядке, и полученное число прибавили к исходному числу. Например, для числа 12345678 получилось после переставления число 78123456 и в сумме – 90469134. Какие числа из промежутка $[46913300; 46913500]$ могли получиться в результате сложения?

4(4) Какие из семизначных чисел вида 7*58*9* (вместо звездочек – пропущенные цифры) делятся на 132?

5(4). Пусть a, b, c, d – попарно различные цифры. Докажите, что если число $\overline{cdcdcdcd}$ не делится на число $\overline{ab}$, то либо число $\overline{cd}$ делится на $\overline{ab}$, либо $\overline{ab} = 73$.

6. (а)(3) Найдите НОД и НОК чисел 2077 и 1608.

(б)(4) Решите диофантово уравнение $2077x - 1608y = 871$.

7. Решите в целых числах уравнения:

(а)(3) $5x^2 + 2xy - 3y^2 = 8$;

*****(б)(5)** $5xy = 3x + 7y$;

*****(в)(5)** $x^3 + y^3 = 8 - x^2y - y^2x$;

*****8(5).** Решите в натуральных числах уравнение:

$$x(x+1) = 4y(y+1).$$

***9(4)** Найдите остаток от деления числа $2013^{2013} + 2014^{2014}$ на 13.