Целые числа

I. Делимость.

Напоминания. (Буквы a, b... обозначают целые числа.) Говорят, что a <u>делится на</u> b, если существует такое c, что $a=b\cdot c$. Вместо " a делится на b " говорят также " a <u>кратно</u> b ", " b <u>делит</u> a ", " b – <u>делитель</u> a ". Пишут так: $a \vdots b$ (читается: a делится на b) и $a \not\vdots\, b$ (a не делится на b).

Верны ли такие утверждения (задачи I – 2):

I. (а) Если $a \vdots c$ и $b \vdots c$, то $a+b \vdots c$ и $a-b \vdots c$. (б) Если $a \not\vdots\, c$ и $b \not\vdots\, c$, то $a+b \not\vdots\, c$. (в) Если $a \not\vdots\, c$ и $b \vdots c$, то $a+b \not\vdots\, c$. (г) Если $ab \vdots c$, то $a \vdots c$ или $b \vdots c$.

2. (а) Если $a \vdots$ I5, $b \vdots$ 2I, то $ab \vdots$ 3I5 (=I5·2I). (б) если $a \vdots$ I5, $a \vdots$ 2I, то $a \vdots$ 3I5.

Докажите (задачи 3 – 6), что

3. Если $a^2 \vdots (a+b)$, то $b^2 \vdots (a+b)$ (Указание. $a^2-b^2= (a+b)(a-b)$.)

4. При любом n число $n(n+1)$ четно (=делится на 2).

5. При любых a и b число a^3+b^3 делится на $a+b$.

6*. При любых n число $7^{2n}-4^{2n}$ делится на 33.

7*. Число a четно и не делится на 4. Доказать, что количество четных делителей числа a равно количеству нечетных делителей числа a (Указание: установить взаимно-однозначное соответствие между чётными и нечётными делителями

2. Остатки.

Напоминания. Пусть a, b – любые (целые) числа, $b>0$. Число a можно разделить с остатком на b, то есть представить в виде $a = k\cdot b + r$, где $0 \le r < b$. Такое представление единственно. Здесь k называется <u>неполным частным</u>, r – <u>остатком</u>.

Пример. Числа 25 и –5 дают при делении на 6 остаток I.

I. Нарисовать все числа от – 20 до 20, дающие остаток 2 при делении на 7.

2. Найти остаток от деления числа (– I50) на I9.

3. При делении I00 на a получили остаток 6. [redacted] Чему может быть равно a? (Дать обоснованный ответ.)

4. Доказать, что (остатки от деления a и b на c равны) $\Leftrightarrow (a-b \vdots c)$

5. Доказать, что числа n и $100n$ дают одинаковые остатки при делении на II.

6. (а) Число a дает при делении на 5 остаток 2, число b – остаток 4. Какие остатки дают (при делении на 5) числа $a+b$ и $a\cdot b$ (ответ и обоснование)?

(б) Заполнить таблицы, указывающие остатки от деления на 5 чисел $a+b$ и $a\cdot b$ (остатки от деления a и b указаны по горизонтали и вертикали).

$b \backslash a$	0	1	2	3	4
0					
1					
2					
3					
4					

Целые числа – 2

Остатки (продолжение)

(в) Какие остатки могут давать точные квадраты при делении на 5 ?
(г)* Доказать, что a^5 и a дают одинаковые остатки при делении на 5. (д) Пользуясь таблицей, докажите, что если $ab \,\vdots\, 5$, то $a \,\vdots\, 5$ или $b \,\vdots\, 5$.

Задача 6 показывает, что для нахождения остатков от деления $a+b$ и $a \cdot b$ на 5 не нужно знать сами a и b : достаточно знать их остатки. (Разумеется, 5 можно заменить на любое число.)

7. Доказать, что любое натуральное число дает такой же остаток при делении на 9, как и сумма его цифр. Вывести отсюда признаки делимости на 9 и на 3.

8. Найти остаток от деления $3n^2+8n+5$ на n при $n = 1, 2, 3, 4, \ldots$

9. Найти остаток (а) от деления 3^{100} на 7; (б) от деления 8^{100} на 7.

10. Было 7 кусков бумаги. Некоторые из них разрезали на 7 кусков. После этого некоторые из получившихся кусков снова разрезали на 7 кусков и так сделали несколько раз. Могло ли получиться 1983 куска?

11. Какой остаток дает число n^2+3n+5 при делении на $n+1$ при $n = 0, 1, 2, 3, \ldots$?

12. Доказать, что из любых 8 целых чисел можно выбрать 2 таких, что их разность делится на 7.

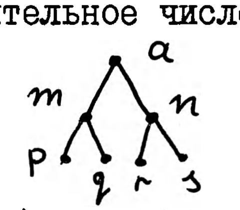
13. (а) Верно ли, что из любых 100 чисел можно выбрать 15 таких, что разность любых двух из выбранных делится на 7 ?
(б) Тот же вопрос для 16 чисел вместо 15. (в) Верно ли, что из 100 чисел всегда можно выбрать 2 таких, у которых сумма делится на 7 ?

14. Может ли число делиться на 8, а при делении на 12 давать остаток 10 ?

15.* Даны 1982 числа. Доказать, что можно выбрать несколько из них так, чтобы сумма выбранных делилась на 1982.

3. Простые числа.

Напоминания. Положительное число p называется простым, если у него нет делителей, кроме ± 1 и $\pm p$ и $p \neq 1$ (Таким образом, 1 не считается простым числом.) Число, не являющееся простым и не равное 1, называется составным. Всякое положительное число можно разложить в произведение простых: если a не простое, то a имеет делитель m, т.е. $a = m \cdot n$; можно считать $m, n > 0$; если



m и n уже простые, то все доказано, если нет, то разложим их дальше и т.д. (Процесс кончится, так как числа уменьшаются!) Как мы докажем впоследствии (п. 6), разложение на простые множители однозначно (любые два разложения одного и того же числа отличаются лишь порядком сомножителей).

I. Найти все простые p, при которых $p+1$ – простое.

2. Петя придумал новую теорему: при всех $n \geqslant 0$ число n^2+n+41 простое. Верна ли его теорема?

3. (а) Найти все простые p, для которых $p+2$ и $p+4$ тоже простые. (б)* Найти все простые p, для которых $p+2$ – простое.

4. Найти все простые p, для которых $p+1$ – точный квадрат.

5. Докажите, что четырехзначное число, не имеющее (одно- и) двузначных делителей, кроме ± 1, простое.

6. (а) Докажите, что числа I00!+2, I00!+3,..., I00!+I00 составные. (I00! = I·2·...·I00). (б) Докажите, что для всякого N имеется N подряд идущих составных чисел.

7*. Докажите, что остаток от деления простого числа на 30 есть простое число или I.

8. (а) Постройте число, которое дает остаток I при делении на любое из чисел от 2 до I00. (б) (Евклид) Докажите, что простых чисел бесконечно много. (Указание. Пусть все простые числа меньше N. Рассмотрите число, дающее остаток I при делении на все числа от 2 до N и получите противоречие.)

<u>4. Наибольший общий делитель. Взаимно простые числа.</u>

Пусть a, b – целые числа. Число d называется <u>общим делителем</u> чисел a и b, если $a \vdots d$, $b \vdots d$. Наибольшее из таких d обозначается НОД(a, b) и называется <u>наибольшим общим делителем</u> чисел a и b. (Если $a = b = 0$, то все числа являются общими делителями a и b и НОД(a, b) не определен.) Числа a и b называются <u>взаимно простыми</u>, если НОД(a, b) = I (т.е. если у a и b нет общих делителей, кроме ± 1).

I. Докажите, что если НОД(a, b) = d, то числа a/d и b/d целые и взаимно просты.

2. Чему равен НОД(a, b), если $a \vdots b$?

3. На числовую ось нанесите точки x, для которых НОД(x, 12) = 2.

4. Какое наибольшее количество одинаковых букетов можно составить из (а) 24 белых и 40 красных георгинов; (б) m белых и n красных георгинов?

5. Докажите, что (а) числа n и $n+1$; (б) числа $n+1$ и $2n+3$ взаимно просты. (Указание. $2n+3 = 2(n+1)+1$.)

6. Доказать, что НОД(a, b) = НОД($a - b$, b).

7. Доказать, что если $1982a = 1983b + 1$, то a и b взаимно просты.

8*. Доказать, что любые два числа в последовательности $2 + 1,\ 2^2 + 1,\ 2^4 + 1,\ 2^8 + 1,\ 2^{16} + 1, \ldots$ взаимно просты. (Указание. $(2^8 - 1) = (2 + 1)(2^2 + 1)(2^4 + 1)$.)

5. Алгоритм Евклида.

Основная лемма. Пусть a, $b > 0$, a дает при делении на b остаток r. Тогда НОД(a, b) = НОД(b, r).

Набросок доказательства. Достаточно доказать, что любой общий делитель пары (a, b) является общим делителем пары (b, r) и наоборот. В самом деле, если $a = bq + r$, $a \vdots d$, $b \vdots d$, то $r = a - bq \vdots d$. Обратно, если $r \vdots d$, $b \vdots d$, то $a = bq + r \vdots d$.

Алгоритм Евклида. Будем называть преобразованием Евклида переход от пары (a, b) с $a > b > 0$ к паре (b, r), где r – остаток от деления a на b. Согласно Основной лемме, преобразование Евклида не меняет наибольшего общего делителя. Поэтому при поисках НОД(a, b) можно использовать преобразование Евклида и искать НОД получившейся пары.

Пример. $(42,30) \longrightarrow (30,12)$ (остаток от деления 42 на 30 равен 12)
$(30,12) \longrightarrow (12,6)$ (остаток от деления 30 на 12 равен 6)
$(12,6) \longrightarrow (6,0)$ (остаток от деления 12 на 6 равен 0)

Поэтому НОД(42,30) = НОД(30,12) = НОД(12,6) = НОД(6,0) = 6.

1. Найти НОД(525,231).

2. Над прямоугольником со сторонами a и b, $a > b$, разрешается делать такую операцию: отрезать квадрат со стороной b. (а) На какие квадраты будет разрезан прямоугольник $141 \cdot 324$ в результате многократного применения этой операции? (б) Доказать, что любой прямоугольник с целыми сторонами будет в конце концов разрезан на квадраты, и найти сторону наименьшего из них. (в)* Верно ли, что любой прямоугольник (не обязательно с целыми сторонами) будет в конце концов разрезан на квадраты?

3. Имеются две большие бочки с водой и две банки на 210 г и 370 г воды. Разрешается наполнять банку в одной бочке и выливать в другую. Используя результаты применения алгоритма Евклида ($(370, 210) \to (210,160) \to (160,50) \to (50,10)$), придумать способ перелить из первой бочки во вторую 160 г, 50г, 10 г. Можно ли с помощью наших банок перелить 75 г ?

4. Блоха прыгает по прямой, совершая короткие прыжки (21 см) и длинные (37 см). Используя алгоритм Евклида, найдите способы, позволяющие блохе сдвинуться на 16 см, 5 см и 1 см.

5. При дележе добычи два фальшивомонетчика, печатавшие бумажки по 2I руб. и 37 руб., решили, что один из них должен другому I руб. Как им рассчитаться, если у обоих есть только напечатанные ими деньги ?

6. Теоретические следствия алгоритма Евклида. Основная теорема арифметики.

I. Пусть $a, b > 0$, d – общий делитель чисел a и b. (а) Докажите, что все числа, получающиеся при применении алгоритма Евклида к паре (a, b), делятся на d. (б) Докажите, что НОД(a, b) делится на d. Из доказанного вытекает такая

Теорема I. Наибольший общий делитель делится на любой другой общий делитель.

2. Пусть $a, b > 0$. Назовем число c хорошим, если можно найти такие целые x и y, что $c = xa + yb$. Таким образом, c хорошее, если
- ковшами в a литров и b литров можно перелить из одной бочки в другую c литров;
- блоха, делающая прыжки в a метров и b метров, может сдвинуться на c метров;
- человек, имеющий только купюры в a рублей и b рублей, может уплатить c рублей другому, у которого имеются такие же купюры.

Докажите, что (I) Числа a и b хорошие; (2) все числа, встречающиеся при применении алгоритма Евклида к (a, b), хорошие; (3) НОД(a, b) – хорошее; (4) все числа, кратные НОД(a, b) – хорошие; (5) всякое хорошее число кратно НОД(a, b). Таким образом, верна

Теорема 2. (Существуют x и y, для которых $c = xa + yb$) $\Leftrightarrow$ $\Leftrightarrow$ (c кратно НОД(a, b)).

Следствие. Если a и b взаимно просты, то существуют x и y, для которых $xa + yb = 1$

3. Докажите, что если $ab \vdots c$ и a взаимно просто с c, то $b \vdots c$, используя следствие из теоремы 2. (Указание. $b = b \cdot 1$; представьте I в виде суммы, пользуясь взаимной простотой a и c.)

4. Докажите, пользуясь утверждением задачи 3, что (а) если $ab \vdots p$ p – простое, то $a \vdots p$ или $b \vdots p$. (б) если $a_1 \cdot \ldots \cdot a_n \vdots p$ p – простое, то $a_i \vdots p$ при некотором i.

5. Докажите единственность разложения на простые множители: если $a = p_1 \cdot \ldots \cdot p_n = q_1 \cdot \ldots \cdot q_m$, то списки $p_1 \ldots p_n$ и $q_1, \ldots, q_m$ состоят из одних и тех же чисел в одинаковом количестве и отличаются лишь порядком. (Указание. Если это не так, то после сокращения всего общего в $p_1, \ldots, p_n$ и $q_1, \ldots, q_m$ мы придем к противоречию с утверждением задачи 4.)

Утверждение о существовании и единственности разложения на множители называется "Основной теоремой арифметики". Оно используется в задачах 6 - 9.

6. Доказать, используя утверждение задачи 5, что если $a \vdots b$, $a \vdots c$, b и c взаимно просты, то $a \vdots bc$.

7*. Известно, что $x^m = y^n$, НОД(m, n) = I. Докажите, что существует такое z, что $x = z^n$, $y = z^m$.

8*. Докажите, что произведение наибольшего общего делителя чисел a и b и наименьшего положительного общего кратного этих же чисел равно $|ab|$.

9*. Докажите, что (а) если p - простое число, то не существует таких (целых) m и n, что $(m/n)^2 = p$; (б) если a - целое число, не являющееся точным квадратом, то не существует таких m и n, что $(m/n)^2 = a$.

7*. Идеалы.

В этом разделе даются другие доказательства теорем I, 2.

Определение. Множество $I \subset \mathbb{Z}$ называется идеалом, если выполнены такие свойства: (И1) $x, y \in I \Rightarrow x+y,\ x-y \in I$

(И2) $x \in I$, n - любое целое число $\Rightarrow nx \in I$.

Примеры идеалов: $\{0\}$, $\mathbb{Z}$, множество четных чисел.

I. Докажите, что если I и J - идеалы, то $I \cap J$ и $I+J = \{i+j \mid i \in I, j \in J\}$ - идеалы.

2. Докажите, что для любого идеала I найдется такое число c, что I = (множество всех кратных числа c). Такое c называется образующей идеала I.

3. Пусть $I = \{x \mid x \vdots a \text{ и } x \vdots b\}$. Докажите, что I - идеал. Пусть c - его образующая. Докажите, что (I) c - общее кратное a и b; (2) если c' - любое общее кратное a и b, то c' кратно c. Таким образом, $|c|$ есть наименьшее общее кратное. Мы получаем также, что

Любое общее кратное двух чисел делится на их наименьшее общее кратное.

4. Пусть $I = \{xa + yb \mid x, y \in \mathbb{Z}\}$. Докажите, что I - идеал. Пусть d - его образующая. Докажите, что (I) d - общий делитель a и b; (2) если d' - любой общий делитель a и b то $d \vdots d'$. (Таким образом, мы получаем, что $|d|$ = НОД(a, b). Выведите отсюда утверждения теорем I и 2 раздела 6.

5. Пусть $ab \vdots c$ и a взаимно просто с c. Докажите, что $b \vdots c$, рассмотрев идеал $\{x \mid xb \vdots c\}$, установив, что он содержит a и c и что его образующая равна I. (Тем самым получено новое решение задачи 3 раздела 6.)

8. Решение уравнений в целых числах.

I. Пользуясь утверждением задачи 3 раздела 6, найдите все целочисленные точки (точки, обе координаты которых целые) на прямой $ax = by$, если (а) $НОД(a,b) = 1$; (б) $НОД(a,b)=d$.

2. Докажите, что если $c \not\vdots НОД(a,b)$, то на прямой $ax+by=c$ нет целочисленных точек, а если $c \vdots НОД(a,b)$, то они есть.

Задача 2 позволяет определить, имеет ли уравнение $ax+by=c$ целочисленные решения. Следующая задача показывает, как их найти. Можно считать, что НОД(a , b) = I (если нет, сократим все члены уравнения на НОД(a , b)).

3. Пусть НОД(a , b) = I. Тогда уравнение $ax+by=c$ имеет бесконечно много целочисленных решений; если x_0, y_0 – одно из них, то все другие можно найти по формулам $x = x_0 + bt$, $y = y_0 - at$ (Докажите.)

4. Найти все решения уравнения $21x - 37y = 1$ (Указание. См. предыдущую задачу и задачи 3 – 5 из раздела 5.)

5. Найти все решения уравнения $21x - 37y = 1982$

6*. Найти все решения уравнений: (а) $105x + 42y = 56$; (б) $-70x + 408y = 34$.

7*. Имеются контейнеры весом I30 кг и I60 кг. Нужно полностью загрузить ими грузовик грузоподъемностью в 3 тонны. Как это можно сделать (указать все решения)?

8*. Найти общую формулу для чисел, дающих остаток 7 при делении на I5 и остаток I2 при делении на 25.

9*. Отметим на числовой прямой точки, дающии при делении на I2 остаток 5, синим карандашом, а точки, дающии при делении на I8 остаток I3 – красным. Каково будет наменьшее расстояние между красной и синей точками?

9*. Разные задачи.

I. Докажите, что если числа a , b , c не имеют общего (не равного ± 1), делителя (т.е. числа, на которое все они делятся), то существуют такие x, y, z , что $xa+yb+zc = 1$.

2. Доказать, что НОД(2^m – I, 2^n – I) = $2^{НОД(m,n)}$ – I.

3. (Китайская теорема об остатках.) Пусть $a_1, \dots, a_n$ – попарно взаимно простые положительные числа, $0 \le r_1 < a_1, \dots, 0 \le r_n < a_n$ Доказать, что существует число A , дающее при делении на a_1 остаток r_1 , при делении на a_2 остаток r_2 и т.д.

4. Пусть применение алгоритма Евклида к паре (a , b) с $a>b$, продолжается n шагов (последним считается тот, в котором остаток равен нулю). Доказать, что a не меньше n-го члена последовательности Фибоначчи 2,3,5,8,I3... (каждый член равен сумме двух предыдущих).

5. Имеется 35 целых чисел. Разрешается одновременно прибавить к любым 23 из них по I. Доказать, что, повторяя эту операцию, можно сделать все числа равными.

6. (Малая теорема Ферма.) Пусть p - простое число, $a \not\vdots\, p$. Доказать, что $a^{p-1} - 1 \,\vdots\, p$

7. Назовем положительное целое число хорошим, если оно есть сум а двух точных квадратов. (Например, $5 = 2^2+1^2$ и $9 = 3^2+0^2$ - хорошие, а 7 - нет.) Докажите, что (а) произведение двух хороших чисел - хорошее; (б) простые числа, дающие остаток 3 при делении на 4 - не хорошие; (в) простые числа, дающие остаток I при делении на 4 - хорошие.

8. Найти все "пифагоровы тройки", то есть все тройки целых чисел x, y и z , для которых $x^2 + y^2 = z^2$.

9. Доказать, что произведение любых n последовательных натуральных чисел делится на $n!$.

IO. Доказать, что существует бесконечно много простых чисел, дающих остаток (а) 3 ; (б) I при делении на 4.