МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА
МАЛЫЙ МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

ЧИСЛА и МНОГОЧЛЕНЫ

Методическая разработка
для учащихся заочного отделения

МОСКВА — 2008

УДК 51(023)
ББК 22.1
Ч67

Ч67 **Числа** и многочлены: Методическая разработка для учащихся заочного отделения ММФ / Автор-составитель А. В. Деревянкин. — М.: Изд-во центра прикладных исследований при механико-математическом факультете МГУ, 2008. — 72 с.: ил.

В разработке рассмотрены основные понятия, связанные с натуральными и целыми числами (деление с остатком, наибольший общий делитель, наименьшее общее кратное, различные системы счисления, простые числа) и многочленами от одной и нескольких переменных.

ББК 22.1

Числа и многочлены.

Автор-составитель А. В. Деревянкин.

Редакторы Д. П. Ильютко, А. Л. Канунников, Е. А. Федосеева.
Техн. редактор М. Ю. Панов.

Издательство ЦПИ при механико-математическом факультете МГУ.
Москва, Воробьёвы горы.

Отпечатано с оригинал-макета на типографском оборудовании механико-математического факультета и франко-русского центра им. А. М. Ляпунова.

Рекомендуем вам, прежде чем приступать к выполнению задания, внимательно прочитать текст параграфов, разобрать приведённые доказательства теорем и решения задач. Над теми задачами из параграфов, решения которых не приведены, подумайте самостоятельно. Такая подготовка поможет вам более успешно выполнить предлагаемое задание.

В брошюре (за исключением раздела «Многочлены») мы будем в основном рассматривать целые и натуральные числа (напомним, что натуральные — это целые положительные числа: 1, 2, 3, . . .). Множество целых чисел обозначается символом $\mathbb{Z}$, множество натуральных чисел — символом $\mathbb{N}$. Используется также обозначение $\mathbb{N}_0$ для множества целых неотрицательных чисел (0, 1, 2, 3, . . .). Символы $\mathbb{Z}$, $\mathbb{N}$ и $\mathbb{N}_0$ часто позволяют сократить запись условия и решения задачи. Например, вместо фразы «m — целое число» можно записать «$m\in\mathbb{Z}$». Знак $\in$ обозначает принадлежность элемента множеству; следовательно, запись «$m\in\mathbb{Z}$» читается так: «элемент m принадлежит множеству $\mathbb{Z}$» или, иначе говоря, «число m является целым». Знак $\notin$ обозначает, что элемент *не принадлежит* множеству: например, запись «$k\notin\mathbb{N}$» означает, что число k не является натуральным.

ДЕЛИМОСТЬ

§ 1. Основные понятия и свойства

О п р е д е л е н и е. Пусть a, $b\in\mathbb{Z}$, причём $b\neq 0$. Число a *делится* на число b, или a *кратно* b (пишут $a\vdots b$), если существует такое $c\in\mathbb{Z}$, что $a=cb$. В этом случае число b называется *делителем* числа a. Если же такого c не существует, то говорят, что a *не делится* на b, или что a *не кратно* b (пишут $a\not\vdots b$)*).

П р и м е р ы: $12\vdots 4$, поскольку $12=3\cdot 4$; $-90\vdots 15$, поскольку $-90=(-6)\cdot 15$; $14\not\vdots 3$, поскольку не существует такого $c\in\mathbb{Z}$, что $14=c\cdot 3$.

Как непосредственно следует из определения делимости, все числа, кратные b, имеют вид cb, где $c\in\mathbb{Z}$.

П р и м е ч а н и е. Используя в дальнейшем записи вида $x\vdots y$, будем всегда полагать, что x, $y\in\mathbb{Z}$ и $y\neq 0$ (если не будет дополнительных условий).

1. Для любого $a\in\mathbb{Z}$ ответьте на вопрос: делится ли a на $-a$?

2. В каком случае для целых чисел a и b одновременно $a\vdots b$ и $b\vdots a$?

Докажем несколько свойств целых чисел, связанных с делимостью (в формулировках свойств буквами будут обозначаться произвольные целые числа).

С в о й с т в о 1. Если $a\vdots c$, $b\vdots c$, то $(a+b)\vdots c$, $(a-b)\vdots c$.

Д о к а з а т е л ь с т в о. Поскольку $a\vdots c$, то существует $m\in\mathbb{Z}$ такое, что $a=mc$. Аналогично, найдётся $n\in\mathbb{Z}$ такое, что $b=nc$. Тогда:

$$a+b=mc+nc=(m+n)c,\quad a-b=mc-nc=(m-n)c.$$

Поскольку $m+n$, $m-n\in\mathbb{Z}$, то это и значит, что $(a+b)\vdots c$, $(a-b)\vdots c$, что и требовалось доказать.

Свойство 1 можно обобщить на случай произвольного количества слагаемых.

*) Если a делится на b, то говорят также, что b *делит* a и обозначают это так: $b|a$. Если же a не делится на b, то говорят, что b *не делит* a и обозначают это так: $b\nmid a$.

С в о й с т в о 1′. Если $a_1\vdots c$, $a_2\vdots c$, ..., $a_n\vdots c$, то $(\pm a_1\pm a_2\pm\ldots\pm a_n)\vdots c$ (вместо любого из знаков «$\pm$» стоит либо «+», либо «−»).

С в о й с т в о 2. Если $a\vdots c$, $b\not\vdots c$, то $(a+b)\not\vdots c$, $(a-b)\not\vdots c$.

Д о к а з а т е л ь с т в о. Предположим, что $(a+b)\vdots c$. Тогда (по свойству 1) $b=((a+b)-a)\vdots c$ (поскольку $(a+b)\vdots c$, $a\vdots c$), что противоречит условию. Следовательно, предположение неверно и $(a+b)\not\vdots c$, что и требовалось доказать. Аналогично можно доказать, что $(a-b)\not\vdots c$.

С в о й с т в о 3. Если $a\vdots b$ и $b\vdots c$, то $a\vdots c$.

С в о й с т в о 4. Если $a\vdots c$, то $(ab)\vdots c$ для любого $b\in\mathbb{Z}$.

3. Докажите свойства 3 и 4.

Упражнения

Во всех задачах этого и последующих разделов (за исключением раздела «Многочлены») буквами обозначены произвольные целые числа, если нет дополнительных условий.

4. Известно, что $a\vdots b$, $c\vdots d$. Докажите, что $(ac)\vdots(bd)$.

5. Докажите, что если $a\vdots b$, то $a^n\vdots b^n$ для любого $n\in\mathbb{N}$.

6. Докажите, что если $a^2\vdots(a+b)$, то и $b^2\vdots(a+b)$.

7. Какие из следующих утверждений верны, а какие — нет? (Верные утверждения необходимо доказать, а для неверных — привести контрпримеры.)

а) Если $a\not\vdots 15$, $b\not\vdots 15$, то $(a+b)\not\vdots 15$. г) Если $a\vdots 15$, $a\vdots 21$, то $a\vdots(15\cdot 21)$.

б) Если $a\vdots 15$, $b\not\vdots 15$, то $(a+b)\not\vdots 15$. д) Если $a\vdots 3$, $b\vdots 7$, то $(ab)\vdots 21$.

в) Если $(ab)\vdots 15$, то $a\vdots 15$ или $b\vdots 15$.

8. Докажите, что если $(2a+3b)\vdots 7$, то и $(a+5b)\vdots 7$.

9. Пусть $(ab)\vdots c$ и $(a+b)\vdots c$. Докажите, что а) $(a^2+b^2)\vdots c$; б) $(a^4+b^4)\vdots c$.

10. Известно, что $(ab+cd)\vdots(a-c)$. Докажите, что и $(ad+bc)\vdots(a-c)$.

11. Известно, что m, n — нечётные числа. Докажите, что $(m^2-n^2)\vdots 8$.

§ 2. Деление с остатком

Пусть дано натуральное число b. Отметим на числовой оси все числа, кратные b. Это будут числа 0, b, $-b$, $2b$, $-2b$, ... (рис. 1). Если

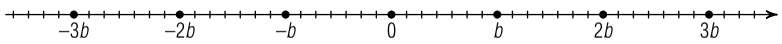

Рис. 1

целое число a совпадает с одним из них, то $a=qb$ (где $q\in\mathbb{Z}$), т. е. a делится на b (см. § 1). Если же a не делится на b, то в этом случае возможно выполнить *деление с остатком*. Предположим, что a распо-

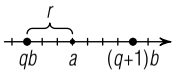

Рис. 2

ложено на числовой оси между числами qb и $(q+1)b$ (рис. 2). Тогда можно записать равенство $a=qb+r$, где, очевидно, $0<r<b$. Отметим, что если a делится на b, то его тоже можно представить в виде $qb+r$, положив $r=0$. Сформулируем теперь определение.

О п р е д е л е н и е. *Разделить с остатком* целое число a на натуральное число b — значит представить a в виде

$$a=qb+r,$$

где $q,\ r\in\mathbb{Z}$ и $0\leqslant r<b$.

Число a называется *делимым*, b — *делителем*, q — *частным**), r — *остатком*.

Подчеркнём ещё раз, что остаток от деления a на b равен 0 тогда и только тогда, когда $a\vdots b$.

Выше мы показали, что деление с остатком всегда возможно, т. е. по данным a, b можно найти частное q и остаток r, удовлетворяющий двойному неравенству $0\leqslant r<b$. Докажем теперь, что деление с остатком всегда можно выполнить единственным способом.

Т е о р е м а 1. Пусть $a\in\mathbb{Z}$, $b\in\mathbb{N}$ и $a=q_1b+r_1=q_2b+r_2$, где q_1, q_2, r_1, $r_2\in\mathbb{Z}$ и $0\leqslant r_1<b$, $0\leqslant r_2<b$. Тогда $q_1=q_2$, $r_1=r_2$.

Д о к а з а т е л ь с т в о. Поскольку $q_1b+r_1=q_2b+r_2$, то $(q_1-q_2)b=r_2-r_1$; следовательно, $(r_2-r_1)\vdots b$. В силу ограничений $0\leqslant r_1<b$, $0\leqslant r_2<b$ имеем: $-b<r_2-r_1<b$. Но из всех целых чисел, удовлетворяющих этому двойному неравенству, только 0 делится на b (почему?); следовательно, $r_2-r_1=0$, или $r_1=r_2$. Тогда из равенства $(q_1-q_2)b=r_2-r_1$ получаем, что $q_1=q_2$. Теорема доказана.

Приведём несколько примеров деления с остатком.

12. Разделите с остатком 100 на 14.

Р е ш е н и е. Очевидно, $100=7\cdot14+2$. Поскольку $0\leqslant2<14$, то данное равенство и выражает результат деления с остатком 100 на 14. Частное в данном случае равно 7, а остаток равен 2. О т в е т: $100=7\cdot14+2$.

13. Разделите с остатком -132 на 5.

Р е ш е н и е. Очевидно, $-132=(-27)\cdot5+3$. Поскольку $0\leqslant3<5$, то в данном случае частное равно -27, а остаток равен 3. О т в е т: $-132=(-27)\cdot5+3$.

З а м е ч а н и е. При решении задачи **13** было бы неправильно записать равенство $-132=(-26)\cdot5+(-2)$ и сделать вывод, что частное равно -26, а остаток равен -2, так как остаток всегда должен быть неотрицательным!

*) Строго говоря, q называется *неполным частным*. Однако слово «неполное» обычно опускают.

Из школы вам хорошо известен способ деления с остатком «в столбик». Однако он годится лишь для случая, когда делимое — положительное число. Следующая задача помогает понять, как быть, если делимое отрицательно.

14. Целое число a даёт при делении на 7 частное q и остаток 2. Какие частное и остаток даёт при делении на 7 число $-a$?

Р е ш е н и е. По условию $a=7q+2$. Тогда $-a=-7q-2=-7\times(q+1)+5=7(-(q+1))+5$. О т в е т: частное равно $-(q+1)$, остаток равен 5.

Как видно из решения приведённой задачи, частное и остаток от деления числа $-a$ на некоторое число b можно определить, если известны частное и остаток от деления a на b.

15. Какой остаток даёт число n^2+3n+5 при делении на $n+1$ (здесь n — произвольное натуральное число)?

Р е ш е н и е. Заметим, что $n^2+3n+5=(n+1)(n+2)+3$. Следовательно, если $n+1>3$ (т. е. $n>2$), то остаток равен 3. Рассмотрим случаи $n=1$ и $n=2$. Если $n=1$, то $n^2+3n+5=9$, $n+1=2$; искомый остаток равен 1. Если же $n=2$, то $n^2+3n+5=15$, $n+1=3$, и искомый остаток равен 0. О т в е т: 1 при $n=1$; 0 при $n=2$; 3 при $n>2$.

Упражнения

16. Разделите с остатком: а) 1005 на 13; б) 1001 на 11; в) 4531945 на 761; г) -150 на 9; д) -54321 на 4.

17. Нарисуйте числовую ось и отметьте на ней все целые числа, лежащие в промежутке от -20 до 20, которые дают остаток 3 при делении на 7.

18. Число a даёт остаток 7 при делении на 10. Чему равен остаток от деления a на 5?

19. Может ли число делиться на 8 и давать остаток 10 при делении на 12?

20. Число a даёт при делении на 9 остаток 5, число b — остаток 8. Какой остаток даёт при делении на 9 число а) $a+b$; б) ab?

21. а) Среди всех чисел, больших 2000 и дающих остаток 4 при делении на 13, найдите наименьшее.

б) Найдите наибольшее число, не превосходящее 10000 и дающее остаток 46 при делении на 94.

22. Найдите наименьшее шестизначное число, которое делится на 321.

23. Число 41 даёт остаток 6 при делении на b. Найдите все возможные значения числа b.

24. Число a даёт остаток 2 при делении на 3 и остаток 1 при делении на 4. Найдите остаток от деления a на 6.

25. Остатки от деления числа n на 3, 5, 7 равны a, b, c соответственно. Докажите, что $(70a+21b+15c-n)\vdots 105$.

26. В одном из подъездов восьмиэтажного дома на первом этаже расположены квартиры с 97 по 102. На каком этаже и в каком подъезде этого дома расположена квартира 178 (все подъезды дома устроены одинаково; на всех этажах одинаковое количество квартир)?

27. Было 10 листов бумаги. Некоторые из них разрезали на 7 частей, и так несколько раз. Могло ли в результате получиться а) 2007 листов; б) 2008 листов?

Указание. Подумайте, как изменяется число листов после каждого разрезания. Запишите, сколько получится листов после n разрезаний.

28. Какой остаток даёт число a при делении на b, где

а) $a=2n^2+5n-3$, $b=n+4$; в) $a=4n+5$, $b=2n+3$;

б) $a=4n+7$, $b=2n+1$; г) $a=n^2+1$, $b=4$,

если n — произвольное натуральное число?

Примечание. Ответ в этой задаче зависит от n. Следует записать его аналогично ответу к задаче **15**.

29. Найдите все целые числа n такие, что значение данного выражения является целым числом:

а) $\dfrac{4n-5}{2n-1}$; б) $\dfrac{2n^2+9n+13}{n+2}$; в) $\dfrac{3n^2+5n+3}{n+2}$.

30. а) Докажите, что из восьми целых чисел всегда можно выбрать два, разность которых делится на 7.

б) Верно ли, что из восьми целых чисел всегда можно выбрать два, сумма которых делится на 7?

в) Докажите, что из пяти целых чисел всегда можно выбрать два, разность квадратов которых делится на 7.

31. Какое наибольшее количество целых чисел можно выбрать, если требуется, чтобы сумма и разность любых двух из них не делилась на 16?

32. Найдите какое-нибудь натуральное число, дающее остаток 1 при делении на 2, остаток 2 при делении на 3, остаток 3 при делении на 4, остаток 4 при делении на 5, остаток 5 при делении на 6, остаток 6 при делении на 7.

33. 1 января 2007 г. пришлось на понедельник. Определите, каким днём недели будет 31 декабря 2050 г.

§ 3. Делители

Напомним, что целое число $b\neq 0$ называется *делителем* целого числа a, если $a\vdots b$. В этом параграфе мы будем рассматривать лишь

натуральные числа и их натуральные делители. Выпишем, например, все делители числа 48:

1, 2, 3, 4, 6, 8, 12, 16, 24, 48.

Несложно заметить, что множество этих делителей обладает определённой симметрией: $1\cdot 48=48$, $2\cdot 24=48$, $3\cdot 16=48$, $4\cdot 12=48$, $6\cdot 8=48$. Это легко объяснить: если число $a\neq 0$ имеет делитель b, то по определению $a=cb$, где $c\in\mathbb{Z}$. Значит, число c тоже является делителем числа a; таким образом, для любого делителя b найдётся парный ему делитель c такой, что произведение b и c равно данному числу a. Такие два делителя называются *дополнительными*. В приведённом примере все делители числа 48 разбиваются на пары дополнительных делителей. Однако так бывает не всегда. Рассмотрим, например, делители числа 36:

1, 2, 3, 4, 6, 9, 12, 18, 36.

Видим, что $1\cdot 36=36$, $2\cdot 18=36$, $3\cdot 12=36$, $4\cdot 9=36$. А вот число 6 осталось без пары. Разгадка проста: ведь $6\cdot 6=36$ — т. е. дополнительным к делителю 6 будет он сам. Подумайте, какое особое свойство числа 36 играет здесь роль (см. ниже задачу **35**).

Упражнения

Во всех задачах этого раздела речь идёт о натуральных числах и их натуральных делителях.

34. Приведите пример натурального числа, имеющего ровно а) 5; б) 6 делителей.

35. Докажите, что число имеет нечётное количество делителей тогда и только тогда, когда оно является полным квадратом*).

36. Пусть a — чётное число, не делящееся на 4. Докажите, что у числа a поровну чётных и нечётных делителей.

37. Докажите, что если натуральное число n имеет s различных делителей, то произведение всех этих делителей равно $\sqrt{n^s}$.

38. Пусть k — количество делителей натурального числа n. Докажите, что $k^2<4n$.

Указание. Разбейте все делители числа n на две группы: в первую отнесите все делители, не превосходящие $\sqrt{n}$, а во вторую — все остальные.

39. Пусть d_1, d_2, ..., d_n — все делители некоторого числа a. Докажите, что если $d_1+d_2+\ldots+d_n=2a$, то $\dfrac{1}{d_1}+\dfrac{1}{d_2}+\ldots+\dfrac{1}{d_n}=2$.

*) *Полный квадрат* (*точный квадрат*) — квадрат некоторого целого числа.

§ 4. Сравнения по модулю

О п р е д е л е н и е. Пусть m — произвольное натуральное число. Два целых числа a и b называются *сравнимыми по модулю m*, если a и b дают одинаковые остатки при делении на m. Пишут $a \equiv b \pmod m$. Если же числа a и b не являются сравнимыми по модулю m, то пишут $a \not\equiv b \pmod m$.

П р и м е р ы: $7 \equiv 13 \pmod 6$; $-8 \equiv 122 \pmod 5$; $40 \not\equiv 0 \pmod 9$.

Разделим a и b с остатком на m: $a = q_1 m + r_1$, $b = q_2 m + r_2$. Если $r_1 = r_2$, то $a - b = q_1 m - q_2 m = ((q_1 - q_2)m) \vdots m$. Обратно, если $(a-b) \vdots m$, т. е. $((q_1 - q_2)m + (r_1 - r_2)) \vdots m$, то и $(r_1 - r_2) \vdots m$. Из определения остатка следуют неравенства $0 \leqslant r_1 < m$, $0 \leqslant r_2 < m$, откуда получаем, что $-m < r_1 - r_2 < m$. Но из всех целых чисел, удовлетворяющих этому двойному неравенству, только 0 делится на m (почему?); следовательно, $r_1 - r_2 = 0$, т. е. $r_1 = r_2$. Таким образом, можно сформулировать определение иначе.

О п р е д е л е н и е. Два целых числа a и b называются *сравнимыми по модулю m*, если $(a-b) \vdots m$.

Рассмотрим основные свойства сравнений по модулю.

Т е о р е м а 2. Если $a \equiv b \pmod m$, $b \equiv c \pmod m$, то $a \equiv c \pmod m$.

Доказательство непосредственно следует из определения (удобнее воспользоваться первой формулировкой).

Т е о р е м а 3. Если $a \equiv b \pmod m$, $c \equiv d \pmod m$, то: 1) $a + c \equiv b + d \pmod m$, $a - c \equiv b - d \pmod m$; 2) $ac \equiv bd \pmod m$.

Д о к а з а т е л ь с т в о. 1) По условию $(a-b) \vdots m$, $(c-d) \vdots m$. Тогда $(a+c) - (b+d) = ((a-b) + (c-d)) \vdots m$, т. е. $a + c \equiv b + d \pmod m$, что и требовалось доказать. Сравнение $a - c \equiv b - d \pmod m$ доказывается аналогично.

2) Выполним преобразования: $ac - bd = ac - bc + bc - bd = (a-b) \times c + b(c-d)$. По условию $(a-b) \vdots m$, $(c-d) \vdots m$; следовательно, и $(ac - bd) \vdots m$, т. е. $ac \equiv bd \pmod m$, что и требовалось доказать.

С л е д с т в и е. Если $a \equiv b \pmod m$, то $a^n \equiv b^n \pmod m$ для любого $n \in \mathbb{N}$.

Как следует из теоремы 3, сравнения по одному и тому же модулю можно складывать, вычитать и умножать. Однако сравнения нельзя делить: так, например, $10 \equiv 2 \pmod 8$, однако $5 \not\equiv 1 \pmod 8$.

Сравнения по модулю бывает удобно использовать при решении задач, связанных с делимостью и остатками. Рассмотрим несколько примеров.

40. Какие остатки может давать квадрат целого числа при делении на 3?

Р е ш е н и е. Рассмотрим произвольное целое число a. В зависимости от того, какой остаток оно даёт при делении на 3, возможны три случая:

1) $a \equiv 0 \pmod 3$. Тогда $a^2 \equiv 0^2 = 0 \pmod 3$.

2) $a \equiv 1 \pmod 3$. Тогда $a^2 \equiv 1^2 = 1 \pmod 3$.

3) $a \equiv 2 \pmod 3$. Тогда $a^2 \equiv 2^2 \equiv 1 \pmod 3$.

Итак, возможны два варианта: $a^2 \equiv 0 \pmod 3$ и $a^2 \equiv 1 \pmod 3$. Это значит, что возможные остатки от деления a^2 на 3 равны 0 и 1. О т в е т: 0; 1.

Решим задачу посложнее.

41. Докажите, что $(12^{2n+1} + 11^{n+2}) \vdots 133$ при любом $n \in \mathbb{N}$.

Р е ш е н и е. Имеем: $12^{2n+1} = 12 \cdot 12^{2n} = 12 \cdot 144^n$. Заметим, что $144 \equiv 11 \pmod{133}$; тогда $144^n \equiv 11^n \pmod{133}$ и $12 \cdot 144^n \equiv 12 \cdot 11^n \pmod{133}$. Далее, $11^{n+2} = 11^2 \cdot 11^n = 121 \cdot 11^n$. Поскольку $121 \equiv -12 \pmod{133}$, то $121 \cdot 11^n \equiv -12 \cdot 11^n \pmod{133}$. Тогда $12 \cdot 144^n + 121 \cdot 11^n \equiv 12 \cdot 11^n + (-12) \times \times 11^n = 0 \pmod{133}$, а это и значит, что $(12^{2n+1} + 11^{n+2}) \vdots 133$, что и требовалось доказать.

Сравнения по модулю позволяют обнаружить интересную закономерность, связанную с остатками степеней целых чисел. Рассмотрим последовательность 2^0, 2^1, 2^2, 2^3, ... Посмотрим, какие остатки дают члены этой последовательности при делении, например, на 5:

$$2^0 = 1, \quad 2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8 \equiv 3 \pmod 5, \quad 2^4 = 16 \equiv 1 \pmod 5,$$
$$2^5 = 32 \equiv 2 \pmod 5, \quad 2^6 = 64 \equiv 4 \pmod 5, \quad 2^7 = 128 \equiv 3 \pmod 5, \quad \ldots$$

Видно, что, начиная с 2^4, остатки начали повторяться. Будут ли они повторяться и дальше? Будут ли они повторяться, если взять другое основание степени вместо 2 или другое число вместо 5? Сравнения по модулю позволяют легко ответить на этот вопрос. Заметим, что поскольку возможных остатков от деления на 5 конечное число, а членов последовательности бесконечно много, то найдутся два члена с одинаковыми остатками. Пусть у n-го и $(n+s)$-го членов последовательности остатки от деления на 5 совпали: $2^n \equiv 2^{n+s} \pmod 5$. Тогда, умножая это сравнение на такое: $2 \equiv 2 \pmod 5$, получим: $2^{n+1} \equiv 2^{(n+1)+s} \pmod 5$. А это значит, что остатки $(n+1)$-го и $((n+1)+s)$-го членов также совпадут. Аналогично получаем, что совпадут и остатки $(n+2)$-го и $((n+2)+s)$-го членов, и т. д. Следовательно, остатки будут повторяться с периодом s.

Поскольку проведённое рассуждение никак не зависит от свойств чисел 2 и 5, то его можно провести и для любых других натуральных чисел. Таким образом, для любых m, $k \in \mathbb{N}$ остатки от деления членов последовательности m^0, m^1, m^2, m^3, ... на k будут периодически повторяться. Длина периода будет зависеть от значений m и k: так, в рассмотренном примере она равна 4. Если, например, положить $m = 3$ и $k = 13$, то длина периода окажется равной 3. Проверьте это самостоятельно.

При некоторых значениях m и k остатки могут периодически повторяться не с самого начала. Например, если $m = 4$ и $k = 120$, то получим следующую последовательность остатков: 1, 4, 16, 64, 16, 64, 16, ...

Рассмотренную закономерность можно применять для решения некоторых задач.

42. Найдите остаток от деления 222^{2007} на 7.

Р е ш е н и е. Поскольку $222=31\cdot7+5$, то $222\equiv5 \pmod 7$, тогда $222^{2007}\equiv5^{2007} \pmod 7$. Найдём остатки от деления на 7 первых нескольких степеней числа 5:

$$5^0=1,\quad 5^1=5,\quad 5^2=25\equiv4 \pmod 7,\quad 5^3=5^2\cdot5\equiv4\cdot5=20\equiv6 \pmod 7,$$
$$5^4=5^3\cdot5\equiv6\cdot5=30\equiv2 \pmod 7,\quad 5^5=5^4\cdot5\equiv2\cdot5=10\equiv3 \pmod 7,$$
$$5^6=5^5\cdot5\equiv3\cdot5=15\equiv1 \pmod 7.$$

Как видно, $5^6\equiv5^0 \pmod 7$, а следовательно, длина периода, с которым повторяются остатки от деления 5^n на 7, равна 6. Это значит, что $5^{6k+r}\equiv5^r \pmod 7$ для любых k, $r\in\mathbb{N}_0$. Заметим, что $2007=334\cdot6+3$; тогда $5^{2007}=5^{334\cdot6+3}\equiv5^3\equiv6 \pmod 7$. О т в е т: 6.

Заметим, что остатки от деления членов последовательности m, $2m$, $3m$, ... на некоторое натуральное k (здесь m — произвольное натуральное число) также циклически повторяются. Доказательство этого факта похоже на приведённое выше доказательство для последовательности m^0, m^1, m^2, m^3, ... Оставляем вам этот вопрос для самостоятельного исследования.

43. Найдите остаток от деления числа 2^{2007} на 3.

Р е ш е н и е. Очевидно, $2\equiv-1 \pmod 3$; следовательно, $2^{2007}\equiv(-1)^{2007}=-1\equiv2 \pmod 3$. Таким образом, искомый остаток равен 2. О т в е т: 2.

Обратите внимание на то, что при решении задачи **43** мы свели основание степени к -1. Сведение основания к 1 или -1 часто упрощает вычисления, поскольку $1^n\equiv1\pmod k$ для любых n, $k\in\mathbb{N}$. При помощи этого приёма можно, например, предложить более простое решение задачи **42**. Заметим, что $5\equiv-2 \pmod 7$; тогда $5^{2007}\equiv(-2)^{2007}=(-1\cdot2)^{2007}=(-1)^{2007}\cdot2^{2007}=-2^{2007} \pmod 7$. Далее, заметим, что $2^3=8\equiv1 \pmod 7$. Тогда $2^{2007}=2^{3\cdot669}=(2^3)^{669}\equiv1^{669}=1 \pmod 7$. Следовательно, $5^{2007}\equiv-2^{2007}\equiv-1\equiv6 \pmod 7$. Таким образом, искомый остаток равен 6.

Докажем ещё одно полезное свойство чисел, которое используется при решении многих задач. Сравнения по модулю позволяют предложить очень компактное и изящное доказательство.

44. Докажите, что $(a^n-b^n)\vdots(a-b)$ при любых $n\in\mathbb{N}$, a, $b\in\mathbb{Z}$, $a\neq b$.

Р е ш е н и е. Положим для определённости, что $a>b$. Очевидно, $(a-b)\vdots(a-b)$, т. е. $a\equiv b \pmod{(a-b)}$. Следовательно, $a^n\equiv b^n \pmod{(a-b)}$, т. е. $(a^n-b^n)\vdots(a-b)$, что и требовалось доказать.

Упражнения

45. Какие остатки может давать полный квадрат при делении на а) 4; б) 5; в) 6; г) 7; д) 8?

46. а) Докажите, что a^2+1 не делится на 3 ни при каком $a\in\mathbb{Z}$.

б) Докажите, что a^2+2 не делится на 5 ни при каком $a\in\mathbb{Z}$.

47. Число a даёт остаток 3 при делении на 5. Чему равен остаток от деления на 5 числа a^2-4a?

48. Докажите, что числа а) 10^4 и 10^6; б) 10^5 и -1; в) -123456789 и 9876543210 дают одинаковые остатки при делении на 11.

49. Докажите, что если a^2+b^2 делится на 7, то числа a и b делятся на 7.

50. Докажите, что число вида 9^n+1, где $n\in\mathbb{N}$, не может оканчиваться более, чем одним нулём.

У к а з а н и е. Используйте сравнения по модулю 4.

51. Имеет ли уравнение $3x^2-4y^2=13$ целочисленные решения?

52. Докажите, что уравнение $x^2+4x-8y=11$ не имеет решений в целых числах.

53. Докажите, что $(2^{5n-2}+5^{n-1}\cdot3^{n+1})\vdots17$ при любом $n\in\mathbb{N}$.

54. Докажите, что $(5^{2n+1}\cdot2^{n+2}+3^{n+2}\cdot2^{2n+1})\vdots19$ при любом $n\in\mathbb{N}_0$.

55. Докажите, что $(1^{2k-1}+2^{2k-1}+\ldots+(2n)^{2k-1})\vdots(2n+1)$ при любых k, $n\in\mathbb{N}$.

56. Найдите остаток от деления числа $7^{100}+11^{100}$ на 13.

57. Найдите последнюю цифру числа 2007^{2007}.

58. На какую цифру оканчивается число 7^{7^7}?

59. Найдите две последние цифры числа 7^{9^9}.

У к а з а н и е. Число, образованное двумя последними цифрами числа n, — это остаток от деления n на 100.

60. Найдите остаток от деления 10! на 13.

П р и м е ч а н и е. Если $n\in\mathbb{N}$, то через $n!$ (читается «эн факториал») обозначается произведение всех натуральных чисел от 1 до n: $n!=1\cdot2\cdot\ldots\cdot n$. Также полагают, что $0!=1$.

61. Докажите, что $(a^n+b^n)\vdots(a+b)$ при любом нечётном $n\in\mathbb{N}$.

62. Докажите, что $(a^{2n}-b^{2n})\vdots(a+b)$ при любом $n\in\mathbb{N}$.

НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ

§ 5. Основные понятия

Рассмотрим два целых числа a и b, хотя бы одно из которых не равно нулю. Выписав все их общие делители, можно найти *наибольший общий делитель*, т. е. наибольшее целое число, которое является делителем как числа a, так и числа b. Наибольший общий делитель чисел a и b обозначается через НОД(a, b), или просто (a, b).

Примеры: НОД$(12, 30)=6$, НОД$(7, -42)=7$, НОД$(15, 22)=1$, НОД$(-10, -24)=2$, НОД$(18, 0)=18$.

Отметим особо, что НОД$(0, 0)$ не определён.

Аналогично формулируется определение наибольшего общего делителя трёх и более чисел, хотя бы одно из которых не равно нулю: это наибольшее целое число, которое является делителем всех данных чисел.

Примеры: НОД$(91, -133, 28, -1001)=7$, НОД$(12, -18, 27)=3$, НОД$(83, 60, 10, 20)=1$.

Если НОД$(a, b)=1$, то числа a и b называются *взаимно простыми*. Один из примеров взаимно простых чисел был приведён выше: 15 и 22. Вот ещё несколько примеров: 9 и 10; -4 и 15; 55 и 87.

Для трёх или более чисел существуют два различных определения.

Определение. Целые числа $a_1, a_2, \ldots, a_n$ называются *взаимно простыми*, если их наибольший общий делитель равен 1.

Определение. Целые числа $a_1, a_2, \ldots, a_n$ называются *попарно взаимно простыми*, если наибольший общий делитель любых двух чисел из этого набора равен 1.

63. Докажите, что если n чисел ($n \geqslant 3$) являются попарно взаимно простыми, то они являются взаимно простыми.

Обратное утверждение неверно: так, например, числа 6, 10, 13 являются взаимно простыми (НОД$(6, 10, 13)=1$), но не являются попарно взаимно простыми, поскольку НОД$(6, 10)\neq 1$.

Упражнения

64. Выберите из следующих чисел все пары взаимно простых чисел: 14, 18, 21, 35, 45, 60, 78, 99.

65. Верно ли, что если НОД$(a, b)=$НОД$(b, c)=d$, то и НОД$(a, c)=d$?

66. Докажите, что если НОД$(a, b)=d$, то НОД $\left(\frac{a}{d}, \frac{b}{d}\right)=1$.

Указание. Предположите, что НОД$(a/d, b/d)>1$, и получите противоречие.

67. Какое наибольшее количество одинаковых букетов можно составить из 192 белых и 264 красных георгинов (нужно использовать все цветы)?

Замечание. В этой задаче наибольшую сложность представляет не получение ответа, а его строгое обоснование!

68. Найдите наибольшее трёхзначное число a, для которого НОД$(a, 540)=36$.

69. а) Известно, что $au+bv=1$. Докажите, что НОД$(a, b)=1$.

б) Известно, что $au+bv=2$. Верно ли, что НОД$(a, b)=2$?

70. Сумма двух натуральных чисел равна 153. Какое наибольшее значение может принимать их наибольший общий делитель?

§ 6. Алгоритм Евклида

Как искать наибольший общий делитель двух данных натуральных чисел? Можно, конечно, действовать по определению: выписать все делители этих чисел, выделить среди них общие и выбрать среди всех общих делителей наибольший. Но этот способ можно порекомендовать лишь для совсем небольших чисел, поскольку он весьма трудоёмок: например, даже для числа 60 поиск всех его делителей может занять несколько минут. А если надо найти НОД$(41450, 3687135)$? В таких случаях гораздо более эффективным оказывается *алгоритм Евклида*, который мы подробно разберём в этом параграфе. Действие алгоритма Евклида основано на приведённых ниже лемме и теореме.

Лемма. Для любых двух целых чисел a и b, хотя бы одно из которых не равно нулю, верно равенство НОД$(a, b)=$НОД$(a-b, b)$.

Доказательство. Покажем, что множество M общих делителей чисел a и b совпадает с множеством N общих делителей чисел $a-b$ и b.

Пусть m — произвольный общий делитель чисел a и b. Тогда $(a-b)\vdots m$ (по свойству 1 из § 1), т. е. m является общим делителем чисел $a-b$ и b.

Обратно, пусть n — произвольный общий делитель чисел $a-b$ и b. Тогда $a=((a-b)+b)\vdots n$ (по свойству 1 из § 1), т. е. n является общим делителем чисел a и b.

Таким образом, множество M общих делителей чисел a и b совпадает с множеством N общих делителей чисел $a-b$ и b; следовательно, и наибольшие элементы этих двух множеств (т. е. НОД(a, b) и НОД$(a-b, b)$) совпадают, что и требовалось доказать.

Сформулируем и докажем теперь теорему, которая, по сути, является обобщением леммы.

Т е о р е м а 4. Пусть $a=qb+r$, где a, b, q, $r\in\mathbb{Z}$, причём хотя бы одно из чисел a, b не равно нулю. Тогда НОД$(a, b)=$НОД(b, r).

Д о к а з а т е л ь с т в о. В соответствии с леммой выполним следующие переходы: НОД$(a, b)=$НОД$(a-b, b)=$НОД$((a-b)-b, b)=$ $=$НОД$(a-2b, b)=\ldots=$НОД$(a-qb, b)=$НОД$(r, b)=$НОД(b, r), что и требовалось доказать.

Итак, пусть даны два натуральных числа a и b и требуется найти их наибольший общий делитель. Положим для определённости, что $a\geqslant b$. Разделим с остатком a на b: пусть $a=bq_1+r_1$. По теореме 4 можно записать: НОД$(a, b)=$НОД(b, r_1). Если $r_1=0$, то НОД$(b, r_1)=$НОД$(b, 0)=$ $=b$, и в этом случае искомый наибольший общий делитель найден. Если же $r_1\neq 0$, то разделим теперь с остатком b на r_1: пусть $b=r_1q_2+r_2$. В силу той же теоремы 4 имеем: НОД$(b, r_1)=$НОД(r_1, r_2). Если $r_2=0$, то искомый наибольший общий делитель равен r_1, если нет — повторяем описанную процедуру, разделив с остатком r_1 на r_2: $r_1=r_2q_3+r_3$, и т. д. Поскольку $b>r_1>r_2>\ldots$ по определению остатка, то процесс конечен, так как все r_i — неотрицательные числа (также по определению остатка).

Описанный алгоритм поиска наибольшего общего делителя двух натуральных чисел и носит название *алгоритма Евклида*. Разберём его применение на примере.

71. Найдите НОД(1014, 273).

Р е ш е н и е. Выполним ряд делений с остатком:

$$\begin{aligned}1014&=273\cdot 3+195;\\ 273&=195\cdot 1+78;\\ 195&=78\cdot 2+39;\\ 78&=39\cdot 2.\end{aligned}$$

По алгоритму Евклида НОД(1014, 273)$=$НОД(273, 195)$=$НОД(195, 78)$=$НОД(78, 39)$=39$. О т в е т: 39.

72. При каких $n\in\mathbb{N}$ числа $3n+1$ и $5n+3$ взаимно просты?

Р е ш е н и е. Согласно лемме, НОД$(3n+1, 5n+3)=$НОД$(3n+1,$ $(5n+3)-(3n+1))=$НОД$(3n+1, 2n+2)=$НОД$((3n+1)-(2n+2), 2n+2)=$ $=$НОД$(n-1, 2n+2)=$НОД$(n-1, (2n+2)-2(n-1))=$НОД$(n-1, 4)$. Очевидно, НОД$(n-1, 4)=1$ тогда и только тогда, когда $(n-1)\not\vdots 2$, т. е. когда n — чётное число. О т в е т: при $n=2k$, где $k\in\mathbb{N}$.

З а м е ч а н и е. Алгоритм Евклида можно применять лишь в случае, когда оба данных числа положительны. Поэтому, если одно (или оба) из чисел a и b, наибольший общий делитель которых нужно найти, отрицательно, то следует воспользоваться очевидным равенством НОД$(a, b)=$ $=$НОД$(|a|, |b|)$, после чего применить алгоритм Евклида к числам $|a|$ и $|b|$.

Т е о р е м а 5. Если НОД$(a, b)=d$, то существуют u, $v\in\mathbb{Z}$ такие, что $au+bv=d$.

Д о к а з а т е л ь с т в о. Запишем равенства, отражающие нахождение НОД(a, b) при помощи алгоритма Евклида:

$$\begin{aligned}a&=bq_1+r_1, &(1)\\ b&=r_1q_2+r_2, &(2)\\ r_1&=r_2q_3+r_3, &(3)\\ r_2&=r_3q_4+r_4, &(4)\\ &\ldots\ldots\ldots\\ r_{n-4}&=r_{n-3}q_{n-2}+r_{n-2}, &(5)\\ r_{n-3}&=r_{n-2}q_{n-1}+r_{n-1}, &(6)\\ r_{n-2}&=r_{n-1}q_n+r_n, &(7)\\ r_{n-1}&=r_nq_{n+1}.\end{aligned}$$

Последний ненулевой остаток — это и есть наибольший общий делитель чисел a и b: $r_n=$НОД(a, b). Перепишем равенства (1)—(7) так, чтобы каждый остаток выражался через два предыдущих:

$$\begin{aligned}r_1&=a-bq_1,\\ r_2&=b-r_1q_2,\\ r_3&=r_1-r_2q_3,\\ r_4&=r_2-r_3q_4,\\ &\ldots\ldots\ldots\\ r_{n-2}&=r_{n-4}-r_{n-3}q_{n-2}, &(8)\\ r_{n-1}&=r_{n-3}-r_{n-2}q_{n-1}, &(9)\\ r_n&=r_{n-2}-r_{n-1}q_n. &(10)\end{aligned}$$

Подставив в равенство (10) выражение для r_{n-1} из (9), получим формулу, выражающую r_n через r_{n-2} и r_{n-3}:

$$r_n=r_{n-2}-r_{n-1}q_n=r_{n-2}-(r_{n-3}-r_{n-2}q_{n-1})q_n=r_{n-2}(1+q_{n-1}q_n)-r_{n-3}q_n.$$

Аналогично выразив в полученном равенстве r_{n-2} через r_{n-3} и r_{n-4} при помощи равенства (8), получим формулу, выражающую r_n через r_{n-3} и r_{n-4}. Затем выразим r_{n-3} через r_{n-4} и r_{n-5}, и т. д. Таким образом мы дойдём до представления r_n в виде $au+bv$, где u, v — некоторые целые числа.

Для примера обратимся к задаче **71**, разобранной выше, и подберём такие u, v, что НОД$(1014, 273)=1014u+273v$:

$$195=1014-273\cdot 3,$$
$$78=273-195\cdot 1,$$
$$39=195-78\cdot 2.$$

Тогда НОД$(1014, 273)=39=195-78\cdot 2=195-(273-195\cdot 1)\cdot 2=273\cdot(-2)+$ $+195\cdot 3=273\cdot(-2)+(1014-273\cdot 3)\cdot 3=1014\cdot 3+273\cdot(-11)$. Итак, $u=3$, $v=-11$.

Следствие из теоремы 5. Если a и b — взаимно простые числа, то существуют u, $v\in\mathbb{Z}$ такие, что $au+bv=1$.

Рассмотрим одно важное свойство наибольшего общего делителя. Например, выпишем все общие положительные делители чисел 180 и 420:

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 10,\ 12,\ 15,\ 20,\ 30,\ 60.$$

Как видно, НОД$(180, 420)=60$. Заметим, что этот наибольший общий делитель делится на любой другой общий делитель чисел 180 и 420. Естественно задаться вопросом: является ли подмеченный факт случайностью или же общей закономерностью, выполняющейся для любой пары чисел? Разберём задачу, дающую ответ на этот вопрос.

73. Докажите, что если $a\vdots c$, $b\vdots c$ и $d=$НОД(a, b), то $d\vdots c$.

Решение. По теореме 5 существуют u, $v\in\mathbb{Z}$ такие, что $au+bv=d$. Из условий $(au)\vdots c$, $(bv)\vdots c$ следует $d=(au+bv)\vdots c$, что и требовалось доказать.

Таким образом, наибольший общий делитель любых двух чисел (хотя бы одно из которых не равно нулю) всегда делится на любой другой общий делитель этих чисел.

Теорема 6. Если $(ab)\vdots c$ и НОД$(a, c)=1$, то $b\vdots c$.

Доказательство. По следствию из теоремы 5 существуют u, $v\in\mathbb{Z}$ такие, что $au+cv=1$. Умножив обе части этого равенства на b, получим: $abu+bcv=b$. По условию $(abu)\vdots c$; кроме того, $(bcv)\vdots c$; следовательно, и $b=(abu+bcv)\vdots c$, что и требовалось доказать.

Теорема 7. Если $ax=by$ $(a,\ b,\ x,\ y\in\mathbb{Z})$ и НОД$(a, b)=1$, то x, y можно представить в виде $x=bt$, $y=at$, где t — некоторое целое число.

Доказательство. Рассмотрим два случая.

1) $b\neq 0$. По условию $(ax)\vdots b$, НОД$(a, b)=1$; следовательно, $x\vdots b$ (по теореме 6), т. е. $x=bt$, где $t\in\mathbb{Z}$. Тогда $y=\dfrac{ax}{b}=\dfrac{abt}{b}=at$.

2) $b=0$. Тогда $a\neq 0$, и исходное уравнение принимает вид $ax=0$, откуда $x=0$. Поскольку НОД$(a, b)=1$, то $a=\pm 1$. Тогда, полагая $t=\dfrac{y}{a}$, имеем: $y=at$, $x=0=0\cdot t=bt$ (число t является целым, поскольку $a=\pm 1$).

Замечание. Заметим, что не только все целочисленные решения уравнения $ax=by$ можно представить в виде $x=bt$, $y=at$, где $t\in\mathbb{Z}$, но и, наоборот, все числа вида $x=bt$, $y=at$, где $t\in\mathbb{Z}$, являются решениями уравнения $ax=by$ (в этом легко убедиться непосредственной подстановкой).

74. Решите в целых числах уравнение $6x+8y=0$.

Решение. Перейдём от данного уравнения к равносильному: $3x=-4y$. Поскольку НОД$(3, -4)=1$, то по теореме 7 все целочисленные решения этого уравнения имеют вид $x=-4t$, $y=3t$, где $t\in\mathbb{Z}$ (и обратно, все числа вида $x=-4t$, $y=3t$ являются решениями данного уравнения). Ответ: $x=-4t$, $y=3t$, где $t\in\mathbb{Z}$.

Теорема 8. Если $a\vdots b$, $a\vdots c$ и НОД$(b, c)=1$, то $a\vdots(bc)$.

Доказательство. По условию $a=qb$, где $q\in\mathbb{Z}$. Тогда $(qb)\vdots c$, НОД$(b, c)=1$; следовательно, $q\vdots c$ (по теореме 6), т. е. $q=kc$, где $k\in\mathbb{Z}$. Тогда $a=qb=(kc)b=k(bc)$, откуда $a\vdots(bc)$, что и требовалось доказать.

75. Докажите, что $(n^3-n)\vdots 6$ при любом $n\in\mathbb{N}$.

Решение. Разложим данное выражение на множители: $n^3-n=$ $=n(n^2-1)=(n-1)n(n+1)$. Заметим, что $n-1$, n и $n+1$ — три последовательных целых числа; одно из них делится на 3 и хотя бы одно — на 2. Следовательно, и все произведение делится на 3 и на 2, а значит, по теореме 8, и на $2\cdot 3=6$, что и требовалось доказать.

Упражнения

76. Найдите наибольший общий делитель чисел: а) 987654321 и 123456789; б) 11111 и 607; в) 16484 и 42282; г) 7777777777 и 777777.

77. От прямоугольника 324×141 отрезают несколько квадратов со стороной 141, пока не останется прямоугольник, у которого одна сторона меньше 141. От полученного прямоугольника снова отрезают квадраты со стороной, равной меньшей стороне этого прямоугольника, до тех пор, пока это возможно, и т. д., пока не останется один квадрат. Сколько квадратов какого размера получится в результате таких операций?

78. Докажите, что НОД$(a, b)=$НОД$(5a+3b, 13a+8b)$ для любых a, $b\in\mathbb{Z}$.

79. При каких натуральных n будут взаимно простыми числа а) $2n+3$ и $n+1$; б) $7n+6$ и $2n+3$; в) n^2+1 и $n+3$?

80. Докажите, что НОД$(n^5+4n^3+3n, n^4+3n^2+1)=1$ при любом $n\in\mathbb{N}$.

81. Найдите все целочисленные решения уравнений а) $6y-21x=0$; б) $78x+143y=0$.

82. Докажите, что если число a не делится ни на 2, ни на 3, то $(a^2-1)\vdots 24$.

83. Докажите, что $(a^5-a)\vdots 30$ при любом $a\in\mathbb{Z}$.

84. На столе лежали книги. Их пытались связывать в пачки по 2, по 3, по 4, по 5 и по 6 штук, но неизменно одна книга оставалась лишней. Когда же книги стали связывать в пачки по 7 штук, то лишних книг не осталось. Какое наименьшее число книг могло быть на столе?

85. Докажите, что $\text{НОД}(2^n-1,\, 2^m-1)=2^{\text{НОД}(m,n)}-1$ для любых $m,\ n\in\mathbb{N}$.

Указание. Докажите сначала равенство $\text{НОД}(2^n-1,\, 2^m-1)=\text{НОД}(2^{n-m}-1,\, 2^m-1)$ (здесь предполагается, что $n\geqslant m$).

86. Докажите, что число $2^{16}+1$ взаимно просто с каждым из чисел 2^1+1, 2^2+1, 2^4+1, 2^8+1.

Указание. Докажите и используйте равенство $2^{16}-1=(2^8+1)(2^4+1)(2^2+1)\times\times(2+1)$.

87. Докажите, что в последовательности

$$2^{2^0}+1,\quad 2^{2^1}+1,\quad 2^{2^2}+1,\quad \ldots,\quad 2^{2^k}+1$$

любые два числа взаимно просты (k — произвольное натуральное число).

88. Найдите наибольший общий делитель всех шестизначных чисел, составленных из цифр 1, 2, 3, 4, 5, 6 (без повторений).

89. а) Даны 35 целых чисел. За одну операцию можно увеличить на 1 любые 23 из этих чисел. Докажите, что за несколько операций можно сделать все числа равными.

б) Даны n целых чисел. За одну операцию можно увеличить на 1 любые m из этих чисел. При каком условии можно за несколько операций сделать все числа равными (при любых начальных значениях этих чисел)?

Примечание. Не забудьте, что требуется не только получить ответ, но и строго доказать, что для всех пар (m, n), вошедших в ответ, все числа действительно можно сделать равными за несколько операций.

§ 7. Диофантовы уравнения

Диофантово уравнение — уравнение с рациональными коэффициентами, для которого поставлена задача поиска решений в целых или рациональных числах.

Простейшим диофантовым уравнением является уравнение

$$ax+by=c, \tag{11}$$

где $a,\ b,\ c\in\mathbb{Z}$ и хотя бы один из коэффициентов a и b не равен нулю.

Как по коэффициентам диофантова уравнения (11) определить, имеет ли оно целочисленные решения? И если имеет, то как найти все эти решения? Ответы на эти вопросы дают приведённые ниже теоремы.

Теорема 9. Уравнение (11), где $a,\ b,\ c\in\mathbb{Z}$ и хотя бы один из коэффициентов a и b не равен нулю, имеет решения в целых числах тогда и только тогда, когда $c\vdots\text{НОД}(a, b)$.

Доказательство. Докажем необходимость; достаточность автоматически будет следовать из дальнейшего изложения.

Пусть уравнение (11) имеет решения в целых числах, и пусть (x_0, y_0) — произвольное целочисленное решение этого уравнения. Тогда $ax_0+by_0=c$. По определению $a\vdots\text{НОД}(a, b)$ и $b\vdots\text{НОД}(a, b)$; тогда и $(ax_0)\vdots\text{НОД}(a, b)$, $(by_0)\vdots\text{НОД}(a, b)$. Следовательно, и $c=(ax_0+by_0)\vdots\text{НОД}(a, b)$, что и требовалось доказать.

Теорема 10. Если $\text{НОД}(a, b)=1$ и (x_0, y_0) — некоторое целочисленное решение уравнения (11), то все решения этого уравнения в целых числах имеют вид

$$\begin{cases} x=x_0-bt,\\ y=y_0+at, \end{cases}$$

где t принимает всевозможные целочисленные значения.

Замечание. Необходимо доказать два утверждения:

1) если (x_1, y_1) — некоторое целочисленное решение уравнения (11), то $x_1,\ y_1$ представляются в виде $x_1=x_0-bt,\ y_1=y_0+at$, где $t\in\mathbb{Z}$;

2) для любого $t\in\mathbb{Z}$ пара (x_0-bt, y_0+at) является решением уравнения (11).

Доказательство теоремы 10. 1) Поскольку пары (x_0, y_0) и (x_1, y_1) являются решениями уравнения $ax+by=c$, то $ax_0+by_0=c$ и $ax_1+by_1=c$, откуда $ax_0+by_0=ax_1+by_1$, или $a(x_0-x_1)=b(y_1-y_0)$. По условию $\text{НОД}(a, b)=1$, тогда (по теореме 7) $x_0-x_1=bt,\ y_1-y_0=at$, где t — некоторое целое число; значит, $x_1=x_0-bt,\ y_1=y_0+at$.

2) Подставив пару (x_0-bt, y_0+at) в уравнение (11), получим: $a(x_0-bt)+b(y_0+at)=ax_0-abt+by_0+abt=ax_0+by_0=c$. Следовательно, эта пара является решением уравнения (11). Теорема доказана.

Таким образом, если известно какое-то одно решение уравнения (11) (как говорят, *частное решение*), то можно записать и все остальные решения. Но как найти хотя бы одно частное решение? Если коэффициенты уравнения малы по модулю, то это решение бывает нетрудно подобрать (например, легко видеть, что пары $(1, -1)$ и $(-2, 3)$ являются решениями уравнения $4x+3y=1$). Но при больших значениях коэффициентов подбор решений может оказаться невыполнимой задачей (попробуйте, например, привести хотя бы одно решение урав-

нения $121x-384y+716=0$), поэтому необходим метод, позволяющий найти частное решение при любых значениях коэффициентов.

Один из таких методов основан на алгоритме Евклида (см. § 6). Алгоритм Евклида позволяет представить НОД(a, b) в виде $au+bv$, где u, v — некоторые целые числа. В данном случае НОД$(a, b)=1$, и, пользуясь упомянутым алгоритмом, можно подобрать такие целые числа u, v, что $au+bv=1$. Тогда $a(uc)+b(vc)=c$; следовательно, пара (uc, vc) является решением уравнения (11).

Рассмотрим нахождение частного решения и применение теоремы 10 на примере.

90. Решите уравнение $84x+65y=4$ в целых числах*).

Р е ш е н и е. Найдём сначала какое-нибудь частное решение данного уравнения. Для этого вычислим НОД(84, 65):

$$\begin{aligned}84&=65\cdot1+19,\\65&=19\cdot3+8,\\19&=8\cdot2+3,\\8&=3\cdot2+2,\\3&=2\cdot1+1,\\2&=1\cdot2.\end{aligned}$$

Следовательно, НОД$(84, 65)=1$; представим этот НОД в виде $84u+65v$:

$$\begin{aligned}19&=84-65\cdot1,\\8&=65-19\cdot3,\\3&=19-8\cdot2,\\2&=8-3\cdot2,\\1&=3-2\cdot1.\end{aligned}$$

Тогда

$$\begin{aligned}1&=3-2\cdot1=\\&=3-(8-3\cdot2)\cdot1=\\&=3\cdot3+8\cdot(-1)=\\&=(19-8\cdot2)\cdot3+8\cdot(-1)=\\&=19\cdot3+8\cdot(-7)=\\&=19\cdot3+(65-19\cdot3)\cdot(-7)=\\&=19\cdot24+65\cdot(-7)=\\&=(84-65\cdot1)\cdot24+65\cdot(-7)=\\&=84\cdot24+65\cdot(-31).\end{aligned}$$

Значит, $4=4\cdot(84\cdot24+65\cdot(-31))=84\cdot96+65\cdot(-124)$. Таким образом, пара $x=96$, $y=-124$ является частным решением данного уравнения.

*) Такое задание подразумевает, что нужно найти в с е целочисленные решения уравнения.

Следовательно, по теореме 10 все целочисленные решения данного уравнения имеют вид $x=96-65t$, $y=-124+84t$, где $t\in\mathbb{Z}$. О т в е т: $x=96-65t$, $y=-124+84t$, где $t\in\mathbb{Z}$.

Теорема 10 даёт решения диофантовых уравнений для случая НОД$(a, b)=1$. А если $d=$НОД$(a, b)\neq1$? Тогда нужно просто разделить обе части уравнения на d: получится равносильное исходному уравнение $\frac{a}{d}x+\frac{b}{d}y=\frac{c}{d}$. Поскольку $c\vdots d$ (иначе по теореме 9 уравнение не имеет решений), то все коэффициенты уравнения останутся целыми, а поскольку НОД $\left(\frac{a}{d}, \frac{b}{d}\right)=1$ (см. задачу **66**), то к полученному уравнению уже можно применить теорему 10.

Отметим, что графиком уравнения $ax+by=c$ является прямая (если хотя бы один из коэффициентов a и b не равен нулю). Целочисленным решениям этого уравнения соответствуют те точки прямой, обе координаты которых — целые числа.

Разберём ещё один тип задач, решаемых с помощью диофантовых уравнений.

91. Найдите общую формулу чисел, дающих при делении на 6 остаток 2, а при делении на 9 — остаток 5.

Р е ш е н и е. По условию искомое число a можно представить в виде $a=6m+2=9n+5$, где m, $n\in\mathbb{Z}$. Следовательно, $6m=9n+3$, или $3n-2m+1=0$. Как несложно видеть, пара $n=1$, $m=2$ является частным решением этого уравнения. Тогда по теореме 10 все его целочисленные решения имеют вид $n=1+2t$, $m=2+3t$, где $t\in\mathbb{Z}$. Таким образом, $a=6m+2=6(2+3t)+2=18t+14$, где $t\in\mathbb{Z}$. О т в е т: $18t+14$, где $t\in\mathbb{Z}$.

У п р а ж н е н и я

92. Имеют ли данные уравнения решения в целых числах:
а) $6x-16y=220$; б) $105x+42y=56$?

93. Решите уравнения в целых числах:
а) $3x-5y=1$; в) $6x+39y+11=0$; д) $43x+250y=7$;
б) $3x+5y=49$; г) $54x-42y+18=0$; е) $11715y-4473x=6390$.

94. Найдите все натуральные n, для которых дробь $\frac{4n+7}{5}$ сократима.

95. Найдите все двузначные числа, которые при делении на сумму своих цифр дают частное 5 и остаток 6.

96. Найдите общую формулу чисел, дающих при делении на 12 остаток 5, а при делении на 30 — остаток 23.

97. Пять одинаковых ручек и семь одинаковых блокнотов стоят 63 руб. Определите цены ручки и блокнота, если эти цены выражаются целым числом рублей.

98. Найдите среди всех целочисленных пар (x, y), составляющих решение уравнения $7x+2y=13$, такую, что $|x+y|$ принимает наименьшее значение.

99. Автомобиль грузоподъёмностью 5 т нужно полностью загрузить контейнерами, имеющими массу 140 кг и 170 кг. Как это можно сделать? Укажите, сколько контейнеров каждого вида следует взять. Не забудьте, что надо найти все решения задачи!

100. На какое наименьшее натуральное число нужно умножить 7, чтобы произведение оканчивалось на 123?

101. Решите систему в целых числах:

$$\begin{cases} 3x+5y-7z=15, \\ 2x+3y-9z=12. \end{cases}$$

102. На числовой оси красным цветом отмечены все числа, дающие при делении на 24 остаток 17; синим цветом — все числа, дающие при делении на 40 остаток 7. Найдите наименьшее расстояние между красной и синей точками.

СИСТЕМЫ СЧИСЛЕНИЯ

§ 8. Десятичная запись

В десятичной системе счисления значение каждой цифры зависит от позиции (разряда), в которой она находится. Например, $32583=3\cdot10^4+2\cdot10^3+5\cdot10^2+8\cdot10^1+3\cdot10^0$, т.е. число 32583 состоит из 3 десятков тысяч, 2 тысяч, 5 сотен, 8 десятков и 3 единиц. Такие системы счисления, в которых значение цифры зависит от позиции, в которой она находится, называются *позиционными*. Поскольку в нашей системе счисления разложение происходит по степеням числа 10, она называется *десятичной*; число 10 называется *основанием системы счисления*.

В общем виде для десятичной системы можно записать:

$$a=\overline{a_1a_2\ldots a_n}=a_1\cdot10^{n-1}+a_2\cdot10^{n-2}+\ldots+a_{n-1}\cdot10^1+a_n\cdot10^0, \qquad (1)$$

где a_1, a_2, $\ldots$, a_n — целые неотрицательные числа, не превосходящие 9, и $a_1\neq0$.

Позже мы познакомимся с позиционными системами счисления, имеющими другие основания (двоичной, шестнадцатеричной и пр.), а также и с непозиционными системами счисления.

103. Найдите все трёхзначные числа, которые в 15 раз больше суммы своих цифр.

Р е ш е н и е. Представим искомое число в виде $\overline{abc}$. По условию $\overline{abc}=15(a+b+c)$, т. е. $100a+10b+c=15(a+b+c)$, или $85a-5b=14c$. Как следует из этого равенства, $(14c)\vdots5$, а значит, по теореме 6, и $c\vdots5$, т. е. $c=0$ или $c=5$. Если $c=0$, то имеем: $85a=5b$, или $17a=b$, что невозможно, поскольку $b\leqslant9$. Следовательно, $c=5$; в этом случае уравнение принимает вид $85a=5b+14\cdot5$, или $17a=b+14$. При $a=1$ имеем $b=3$; если же $a\geqslant2$, то $b\geqslant17\cdot2-14=20$, чего не может быть. О т в е т: 135.

Упражнения

104. Целое число a оканчивается цифрой 5. Докажите, что a^2 оканчивается на 25.

105. Квадрат целого числа оканчивается двумя одинаковыми цифрами. Какими? (Укажите все возможные варианты и докажите, что других нет.)

106. Найдите все трёхзначные числа, которые в 14 раз больше суммы своих цифр.

107. Существует ли целое число, которое при зачеркивании первой цифры уменьшается а) в 36 раз; б) в 38 раз?

§ 9. Признаки делимости

Для того, чтобы узнать, делится ли некоторое натуральное число a на натуральное число b, можно просто разделить a на b (например, «в столбик») и посмотреть, будет ли остаток равен 0. Однако, если число a велико, то такое деление может оказаться достаточно трудоёмким. В связи с этим возникает вопрос: можно ли, не выполняя деления, определить по десятичной записи чисел a и b, делится ли a на b? Во многих случаях ответ на этот вопрос оказывается утвердительным.

Признак делимости на 2. Натуральное число делится на 2 тогда и только тогда, когда его последняя цифра делится на 2.

Замечание. Так как в формулировке фигурируют слова «тогда и только тогда», то этот признак представляет собой два утверждения:

1) если число делится на 2, то его последняя цифра делится на 2;

2) если последняя цифра числа делится на 2, то и само число делится на 2.

Для доказательства признака необходимо показать справедливость обоих утверждений (либо доказав каждое по отдельности, либо проведя рассуждение, доказывающее сразу оба утверждения).

Перед тем, как доказывать признак делимости на 2, рассмотрим лемму, которая окажется полезной при доказательстве как этого, так и других признаков.

Лемма. Пусть $(k-l)\vdots n$. В этом случае $k\vdots n$ тогда и только тогда, когда $l\vdots n$.

Доказательство. По условию $k-l=tn$, где $t\in\mathbb{Z}$. Тогда, если $k\vdots n$, то и $l=(k-tn)\vdots n$ по свойству 1 из § 1. Обратно, если $l\vdots n$, то и $k=(l+tn)\vdots n$ по свойству 1 из § 1. Лемма доказана.

Доказательство признака делимости на 2. Перенесём в равенстве (1) слагаемое $a_n\cdot 10^0$ в левую часть:

$$a-a_n=a_1\cdot 10^{n-1}+a_2\cdot 10^{n-2}+\ldots+a_{n-1}\cdot 10^1=$$
$$=10(a_1\cdot 10^{n-2}+a_2\cdot 10^{n-3}+\ldots+a_{n-1}\cdot 10^0).$$

Число, стоящее в правой части, делится на 2; значит, $(a-a_n)\vdots 2$. Следовательно, $a\vdots 2$ тогда и только тогда, когда $a_n\vdots 2$ (согласно лемме), что и требовалось доказать.

Похожие формулировки имеют и некоторые другие признаки делимости.

Признак делимости на 4. Натуральное число делится на 4 тогда и только тогда, когда число, образованное двумя его последними цифрами, делится на 4.

Признак делимости на 8. Натуральное число делится на 8 тогда и только тогда, когда число, образованное тремя его последними цифрами, делится на 8.

Признак делимости на 5. Натуральное число делится на 5 тогда и только тогда, когда его последняя цифра делится на 5 (т. е. равна 5 или 0).

Признак делимости на 10. Натуральное число делится на 10 тогда и только тогда, когда его последняя цифра равна 0.

Признак делимости на 25. Натуральное число делится на 25 тогда и только тогда, когда две его последние цифры — нули или образуют число, делящееся на 25 (т. е. 25, 50 или 75).

Признак делимости на 50. Натуральное число делится на 50 тогда и только тогда, когда оно оканчивается на 00 или 50.

Признак делимости на 100. Натуральное число делится на 100 тогда и только тогда, когда две его последние цифры — нули.

Другую группу составляют признаки делимости на 3 и на 9.

Признак делимости на 3. Натуральное число делится на 3 тогда и только тогда, когда сумма его цифр делится на 3.

Признак делимости на 9. Натуральное число делится на 9 тогда и только тогда, когда сумма его цифр делится на 9.

Признак делимости на 11 формулируется более сложно.

Признак делимости на 11. Пусть S_1 — сумма цифр, стоящих в натуральном числе a на нечётных местах, а S_2 — сумма цифр, стоящих в числе a на чётных местах. Число a делится на 11 тогда и только тогда, когда $(S_1-S_2)\vdots 11$.

Признаки делимости на 3, 9 и 11 легко доказать, используя сравнения по модулю. Докажем, например, признак делимости на 3.

Доказательство признака делимости на 3. Поскольку $10\equiv 1 \pmod 3$, то $10^n\equiv 1^n=1 \pmod 3$ при любом $n\in\mathbb{N}$. Тогда $\overline{a_1a_2\ldots a_n}=a_1\cdot 10^{n-1}+a_2\cdot 10^{n-2}+\ldots+a_{n-1}\cdot 10^1+a_n\cdot 10^0\equiv a_1\cdot 1+a_2\cdot 1+\ldots+a_{n-1}\cdot 1+a_n=a_1+a_2+\ldots+a_{n-1}+a_n \pmod 3$.

Мы получили, что любое натуральное число сравнимо с суммой своих цифр по модулю 3, а это и значит (согласно лемме), что число делится на 3 тогда и только тогда, когда сумма его цифр делится на 3.

Из рассмотренных признаков можно получить ещё несколько признаков делимости. Рассмотрим, например, признак делимости на 6. Очевидно, если число делится на 6, то оно делится на 2 и на 3. Обратно, если число делится на 2 и на 3, то, согласно теореме 8, оно делится и на 6.

Признак делимости на 6. Натуральное число делится на 6 тогда и только тогда, когда оно делится на 2 и на 3 одновременно.

Подобным образом можно получить много новых признаков делимости, используя признаки, сформулированные в этом параграфе.

108. Сформулируйте признаки делимости на 12, 15, 18, 30, 45, 60.

Отметим, что существуют и другие признаки делимости (на 7, на 13, на 19 и другие числа), но они формулируются и доказываются более сложно, чем рассмотренные выше. Вообще, используя сравнения по модулю, можно вывести признак делимости на любое натуральное число, однако большинство таких признаков оказываются очень неудобными в практическом использовании и представляют скорее теоретический интерес.

Упражнения

109. Докажите сформулированные в этом параграфе признаки делимости а) на 8; б) на 11.

110. а) Найдите все числа вида $\overline{34x5y}$, которые делятся на 36.

б) Найдите все числа вида $\overline{71x1y}$, которые делятся на 45.

111. К числу 15 припишите слева и справа по одной цифре так, чтобы получившееся число делилось на 15.

112. а) Докажите, что число $\overline{a_0a_1a_2a_3}$ делится на 99 тогда и только тогда, когда число $\overline{a_0a_1}+\overline{a_2a_3}$ делится на 99.

б) Докажите, что число $\overline{a_0a_1a_2a_3}$ делится на 101 тогда и только тогда, когда $\overline{a_0a_1}=\overline{a_2a_3}$.

113. Докажите, что число $\overline{a_0a_1a_2}$ делится на 8 тогда и только тогда, когда число $\overline{a_0a_1}+\dfrac{a_2}{2}$ делится на 4.

114. В натуральном числе a переставили цифры, в результате чего оно уменьшилось в три раза. Докажите, что $a\vdots 27$.

115. В натуральном числе a переставили цифры, в результате чего получилось число b. Докажите, что $(a-b)\vdots 9$.

Указание. Используйте идею доказательства признака делимости на 3.

116. Найдите наименьшее число, делящееся на 4, в записи которого встречаются все десять цифр.

§ 10. Различные системы счисления

Система счисления — это совокупность правил записи и чтения чисел. Мы привыкли записывать числа в десятичной системе счисления. В § 8 было объяснено, что это значит. Однако в качестве основания системы счисления можно взять любое натуральное число, большее 1. В общем виде для системы счисления с основанием p можно записать*):

$$(\overline{a_1a_2\ldots a_n})_p=a_1\cdot p^{n-1}+a_2\cdot p^{n-2}+\ldots+a_{n-1}\cdot p^1+a_n\cdot p^0,$$

где a_1, a_2, ..., a_n могут принимать значения 0, 1, 2, ..., $p-1$: в системе счисления с основанием p используются p цифр.

117. Переведите число 3201313 из четверичной системы счисления в десятичную.

Решение. $3201313_4=3\cdot4^6+2\cdot4^5+0\cdot4^4+1\cdot4^3+3\cdot4^2+1\cdot4^1+3\cdot4^0=$
$=(((((3\cdot4+2)\cdot4+0)\cdot4+1)\cdot4+3)\cdot4+1)\cdot4+3=((((14\cdot4+0)\cdot4+1)\times$
$\times4+3)\cdot4+1)\cdot4+3=(((56\cdot4+1)\cdot4+3)\cdot4+1)\cdot4+3=((225\cdot4+3)\cdot4+1)\times$
$\times4+3=(903\cdot4+1)\cdot4+3=3613\cdot4+3=14455$. Ответ: 14455.

Отметим, что можно было бы провести вычисления и по-другому, вычислив сперва все степени числа 4 вплоть до 4^6 и затем посчитав сумму $3\cdot4^6+2\cdot4^5+0\cdot4^4+1\cdot4^3+3\cdot4^2+1\cdot4^1+3\cdot4^0$.

Разберём на примере перевод числа из десятичной системы счисления в какую-либо другую.

118. Переведите число 2238 в семеричную систему счисления.

Решение. Предположим,

$$2238=(\overline{a_1a_2\ldots a_n})_7=a_1\cdot7^{n-1}+a_2\cdot7^{n-2}+\ldots+a_{n-1}\cdot7^1+a_n\cdot7^0.$$

Заметим, что

$$a_1\cdot7^{n-1}+a_2\cdot7^{n-2}+\ldots+a_{n-1}\cdot7^1+a_n\cdot7^0=$$
$$=7\cdot(a_1\cdot7^{n-2}+a_2\cdot7^{n-3}+\ldots+a_{n-1}\cdot7^0)+a_n;$$

следовательно, $a_1\cdot7^{n-2}+a_2\cdot7^{n-3}+\ldots+a_{n-1}\cdot7^0$ — это частное, a_n — остаток от деления числа 2238 на 7. Запишем: $2238=319\cdot7+5$. Таким образом, $a_n=5$, $a_1\cdot7^{n-2}+a_2\cdot7^{n-3}+\ldots+a_{n-1}\cdot7^0=319$. Аналогично получаем, что $a_1\cdot7^{n-3}+a_2\cdot7^{n-4}+\ldots+a_{n-2}\cdot7^0$ — частное, a_{n-1} — остаток от деления 319 на 7. Поскольку $319=45\cdot7+4$, то $a_{n-1}=4$, $a_1\cdot7^{n-3}+a_2\cdot7^{n-4}+\ldots+a_{n-2}\cdot7^0=45$. Выполнив аналогичные действия, получим, что $a_{n-2}=3$, $a_1\cdot7^{n-4}+a_2\cdot7^{n-5}+\ldots+a_{n-3}\cdot7^0=6$. Это значит, что $n=4$, $a_1=a_{n-3}=6$. Итак, $2238=6345_7$. Ответ: 6345.

*) Основание системы, в которой записано число, указывают справа от этого числа. При записи числа в десятичной системе основание, как правило, не указывают.

Проведённые вычисления можно было записать при помощи деления «в столбик»:

$$\begin{array}{r|l} 2238 & 7 \\ \hline 21 & 319 \\ \hline 13 & 28 \\ 7 & 39 \\ \hline 68 & 35 \\ 63 & 4 \\ \hline 5 & \end{array} \qquad \begin{array}{r|l} 7 & \\ \hline 319 & 7 \\ \hline 45 & 7 \\ \hline 42 & \mathbf{6} \\ \hline \mathbf{3} & \end{array}$$

На основании решения задачи **118** можно сформулировать алгоритм перевода натурального числа N из десятичной системы счисления в систему с основанием n.

1) Разделим N на n с остатком: $N=N_1n+r_1$. Последняя цифра искомого числа равна r_1.

2) Разделим N_1 на n с остатком: $N_1=N_2n+r_2$. Предпоследняя цифра искомого числа равна r_2.

3) Разделим N_2 на n с остатком, и т. д. до тех пор, пока очередное полученное частное N_k не станет равно 0.

В электронно-вычислительных машинах широко используется двоичная система счисления. В ней всего две цифры: 0 и 1. Например, $1011101_2=1\cdot2^6+1\cdot2^4+1\cdot2^3+1\cdot2^2+1\cdot2^0=64+16+8+4+1=93$. Менее распространена шестнадцатеричная система счисления, также используемая в вычислительной технике. В ней используются 16 цифр: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. При этом:

$$\begin{array}{llll} 0_{16}=0_{10}, & 4_{16}=4_{10}, & 8_{16}=8_{10}, & C_{16}=12_{10}, \\ 1_{16}=1_{10}, & 5_{16}=5_{10}, & 9_{16}=9_{10}, & D_{16}=13_{10}, \\ 2_{16}=2_{10}, & 6_{16}=6_{10}, & A_{16}=10_{10}, & E_{16}=14_{10}, \\ 3_{16}=3_{10}, & 7_{16}=7_{10}, & B_{16}=11_{10}, & F_{16}=15_{10}. \end{array}$$

Например,

$$BC8_{16}=11\cdot16^2+12\cdot16^1+8\cdot16^0=11\cdot256+12\cdot16+8=3016.$$

Ещё более ограниченное применение в вычислительных машинах находят восьмеричная и троичная системы счисления. Некоторые другие системы счисления (пятеричная, двенадцатеричная, двадцатеричная, шестидесятеричная) были в древности распространены у различных народов мира. До наших дней дошло, например, комплектование столовой посуды дюжинами и деление часа на 60 минут.

Арифметические действия в системах с любым основанием проводятся по одной и той же схеме. Главным принципом является то, что n единиц какого-либо разряда составляют одну единицу следующего, более старшего разряда (здесь n — основание системы), например: $4_7+3_7=10_7$, $60_9+30_9=100_9$.

Разберём примеры на сложение и умножение чисел.

119. Вычислите $37267_8+55143_8$, $2765_8\cdot736_8$.

Р е ш е н и е. Составим таблицы сложения и умножения для восьмеричной системы (при решении подобных задач составление таких таблиц не требуется; здесь они приведены лишь для наглядности):

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	10
2	2	3	4	5	6	7	10	11
3	3	4	5	6	7	10	11	12
4	4	5	6	7	10	11	12	13
5	5	6	7	10	11	12	13	14
6	6	7	10	11	12	13	14	15
7	7	10	11	12	13	14	15	16

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	10	12	14	16
3	0	3	6	11	14	17	22	25
4	0	4	10	14	20	24	30	34
5	0	5	12	17	24	31	36	43
6	0	6	14	22	30	36	44	52
7	0	7	16	25	34	43	52	61

Теперь приступим к вычислениям:

$$\begin{array}{r} 37267 \\ +\ 55143 \\ \hline 114432 \end{array} \qquad \begin{array}{r} 2765 \\ \times\ 736 \\ \hline 21676 \\ 10737 \\ \underline{24663} \\ 2617566 \end{array}$$

О т в е т: 114432; 2617566.

По аналогии с десятичной системой счисления производится и деление. Вот пример, выражающий запись деления одного числа на другое в восьмеричной системе счисления:

$$\begin{array}{r|l} 1657 & 5 \\ \hline 12 & 274 \\ \hline 45 & \\ 43 & \\ \hline 27 & \\ 24 & \\ \hline 3 & \end{array}$$

Таким образом, в восьмеричной системе счисления $1657=274\cdot5+3$.

Отметим, что все разобранные в § 9 признаки делимости годятся лишь для десятичной системы счисления. Понятно, почему: ведь эти признаки используют цифровую запись числа, а одно и то же число может в разных системах счисления записываться разными цифрами. Для каждой системы счисления можно получить свои признаки делимости.

Все рассмотренные до сих пор системы счисления относятся к *позиционным*. Однако существуют ещё и *непозиционные* системы счисления, в которых значение каждой цифры не зависит от того, в какой позиции она расположена. К таким системам относится известная вам *римская* система счисления. Её цифры имеют следующие значения: I — 1, V — 5, X — 10, L — 50, C — 100, D — 500, M — 1000. Если цифра идёт после более старших цифр, то она прибавляется к общей сумме; если же цифра встречается перед более старшей цифрой, то она вычитается из общей суммы. Примеры: XXXVII$=10+10+10+5+1+1=37$, CXCIV$=100+100-10+5-1=194$.

Другими примерами непозиционных систем счисления являются древнегреческая, египетская, славянская, не употребляемые в настоящее время. Непозиционные системы счисления являются менее удобными, чем позиционные, поскольку в них сложно выполнять арифметические действия, а записи больших чисел получаются очень громоздкими. В связи с этим десятичная система счисления, возникшая в Индии*), практически полностью вытеснила в средние века все непозиционные системы.

Упражнения

120. Переведите числа из двоичной системы счисления в десятичную: а) 1001011; б) 11111111.

121. Переведите числа из шестнадцатеричной системы счисления в десятичную: а) 1E2; б) ABC; в) 7D90F.

122. Переведите числа из десятичной системы счисления в двоичную: а) 1000; б) 2007; в) 123456.

123. Переведите числа из десятичной системы счисления в шестеричную: а) 1000; б) 5000; в) 45678.

124. Выполните действия, не переводя числа в десятичную систему счисления:

а) $101110_2+1100111_2$;
б) $2112001_3+22001012_3$;
в) $10010011_3-2210022_3$;
г) $ABCD_{16}+DCBA_{16}$;
д) $343224_7\cdot 125_7$;
е) $34112_5\cdot 3444_5$;
ж) $34718_{12}\cdot 26_{12}$;
з) $54321_6:253_6$.

*) Существующее ныне название «арабская» объясняется тем, что европейцы позаимствовали десятичнную систему у арабов, к которым она пришла из Индии.

125. Сравните, не переводя числа из одной системы счисления в другую, 14387_9 и 14387_{12}.

126. Найдите n, если $1241_5=304_n$.

127. Докажите, что число 144_n является полным квадратом при любом $n\geqslant 5$.

128. В каких системах счисления справедливы равенства: а) $3\cdot 4=10$; б) $10+10+10=100$; в) $15^2=321$?

129. Найдите a, b, c, если $\overline{abc}_5=\overline{cba}_8$.

130. На доске написано число 1. С написанным числом разрешается выполнить одну из следующих двух операций:

1) умножить его на 2;

2) умножить его на 2 и прибавить 1.

Сколькими способами можно при помощи этих операций получить за несколько шагов число 1000?

131. Докажите признак делимости: число, записанное в троичной системе, тогда и только тогда делится на 2, когда сумма его цифр делится на 2.

132. На доске сохранилась полустёртая запись, выражающая сложение двух чисел в столбик (стёртые цифры заменены звёздочками):

$$\begin{array}{r} 23*5* \\ +\ 1*642 \\ \hline 42423 \end{array}$$

Определите, в какой системе счисления записаны числа, и восстановите пример.

133. В наборе имеется по одной гирьке массы 1 г, 2 г, 4 г, 8 г, 16 г, 32 г, 64 г. Докажите, что при помощи этих гирек можно уравновесить груз любой целочисленной массы от 1 г до 127 г (гирьки можно класть только на одну чашу весов!).

Указание. Запишите все массы в двоичной системе счисления.

ПРОСТЫЕ ЧИСЛА

Простые числа играют очень важную роль при изучении целых чисел: как вы увидите ниже, это своеобразные «кирпичики», из которых составляются все остальные целые числа. С помощью разложения на простые множители можно получить наглядные решения самых разных задач.

В этом разделе мы будем рассматривать лишь натуральные числа, если не будет дополнительных условий.

§ 11. Основные понятия

Зададимся вопросом: сколько делителей имеют различные натуральные числа? Любое число, большее 1, имеет по крайней мере два делителя: 1 и само это число. Некоторые числа имеют и другие делители (так, число 10 имеет ещё делители 2 и 5; число 9 имеет ещё делитель 3).

Определение. Числа, не имеющие положительных делителей, кроме единицы и самого себя, называются *простыми*. Числа, имеющие, кроме единицы и самого себя, ещё хотя бы один положительный делитель, называются *составными*.

Единицу не относят ни к простым, ни к составным числам.

Это определение можно сформулировать иначе.

Определение. Числа, имеющие ровно два положительных делителя, называются *простыми*. Числа, имеющие более двух положительных делителей, называются *составными*.

Познакомимся ещё с одним интересным понятием, связанным с простыми числами. *Числа-близнецы* — два простых числа, разность между которыми равна 2, например: 3 и 5, 5 и 7, 17 и 19, 2027 и 2029.

Упражнения

134. Число p — простое. Докажите, что для любого $a\in\mathbb{Z}$ либо $a\vdots p$, либо НОД$(a, p)=1$.

135. Пусть p и $p+2$ — два простых числа-близнеца ($p>3$). Докажите, что $(p+1)\vdots 6$.

136. Найдите все простые числа p такие, что $p+1$ — полный квадрат.

137. Сумма двух целых чисел равна 101, а разность их квадратов — простое число. Найдите эти числа.

138. Докажите, что число $\underbrace{55\ldots53}_{2007}$ — составное.

139. Докажите, что найдутся 1000 идущих подряд составных чисел.

140. Докажите, что если $((m-1)!+1)\vdots m$, где $m>1$, то m — простое.

141. Докажите, что если число p — простое и $p>5$, то либо $p^2\equiv 1 \pmod{30}$, либо $p^2\equiv 19 \pmod{30}$.

142. Даны два различных простых числа p и q. Сколько существует целых чисел от 1 до pq включительно, не делящихся ни на p, ни на q?

§ 12. Разложение на простые множители

Пусть дано некоторое составное число a. Его можно разложить в произведение двух множителей, отличных от 1 и a: $a=bc$, где $1<b<a$, $1<c<a$. Если числа b и c простые, то мы получили разложение числа a на простые множители. Если же хотя бы одно из них составное, то его тоже можно разложить на два множителя. Если среди полученных множителей окажутся составные, разложим и их, и т. д. до тех пор, пока не останутся только простые множители $p_1, p_2, \ldots, p_n$ (подумайте, почему это рано или поздно произойдёт). В результате получим разложение числа a на простые множители: $a=p_1p_2\cdot\ldots\cdot p_n$. Поясним описанный алгоритм на примере.

143. Разложите число 240 на простые множители.

Решение. $240=12\cdot20=(3\cdot4)\cdot(4\cdot5)=(3\cdot2\cdot2)\cdot(2\cdot2\cdot5)=2\cdot2\cdot2\cdot2\cdot3\cdot5=2^4\cdot3\cdot5$. Ответ: $240=2^4\cdot3\cdot5$.

Обратите внимание на то, что мы записали ответ в *каноническом виде*: собрали вместе одинаковые простые множители и упорядочили все простые множители по возрастанию.

В общем виде каноническое разложение числа N на простые множители выглядит следующим образом:

$$N=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_n^{\alpha_n}, \qquad (1)$$

где $p_1, p_2, \ldots, p_n$ — различные простые числа, упорядоченные по возрастанию ($p_1<p_2<\ldots<p_n$), $\alpha_i\in\mathbb{N}$ ($1\leqslant i\leqslant n$).

Отметим, что при необходимости можно дополнить каноническое разложение простыми множителями, не входящими в разложение числа N, записав их в нулевых степенях (так как $p^0=1$ для любого $p\in\mathbb{N}$): например, в рассмотренной задаче можно было представить число 240 в виде $2^4\cdot3\cdot5\cdot7^0$ или $2^4\cdot3\cdot5\cdot11^0\cdot17^0$. Поэтому можно полагать, что в каноническом разложении (1) $\alpha_i\in\mathbb{N}_0$ $(1\leqslant i\leqslant n)$. Подобным образом часто поступают при рассмотрении разложений нескольких различных чисел на простые множители. Тогда целесообразно включать в множество $\{p_1, p_2, \ldots, p_n\}$ все простые числа, которые входят в разложение хотя бы одного из данных чисел. Например, разложения чисел $a=2^2\cdot3^6\cdot7$ и $b=3^4\cdot5\cdot11^2$ можно записать так:

$$a=2^2\cdot3^6\cdot5^0\cdot7\cdot11^0, \qquad b=2^0\cdot3^4\cdot5\cdot7^0\cdot11^2.$$

Рассмотренный выше алгоритм позволяет разложить любое составное число на простые множители. Однако возникает вопрос: а единственно ли такое разложение? Например, в задаче **143** можно было выделять множители по-другому: $240=4\cdot60$, или $240=2\cdot120$, или $240=24\cdot10\ldots$ (для числа 240 уже на первом шаге существует 18 различных способов). Вдруг иная последовательность действий привела бы нас к другому результату?

Оказывается, нет. Разложение числа на простые множители всегда единственно; два разложения одного и того же числа могут различаться лишь порядком множителей. Этот факт интуитивно кажется очевидным, однако нуждается в строгом доказательстве. Сначала докажем лемму.

Лемма. Пусть $p_1, p_2, \ldots, p_n, q$ — простые числа и $(p_1p_2\cdot\ldots\cdot p_n)\vdots q$. Тогда хотя бы одно из чисел $p_1, p_2, \ldots, p_n$ совпадает с q.

Доказательство. Если $p_n\vdots q$, то $p_n=q$, иначе p_n окажется составным (почему?). Если же $p_n\not\vdots q$, то по задаче **134** НОД$(p_n, q)=1$ и тогда, поскольку $((p_1p_2\cdot\ldots\cdot p_{n-1})p_n)\vdots q$, то $(p_1p_2\cdot\ldots\cdot p_{n-1})\vdots q$ в силу теоремы 6. Если $p_{n-1}\vdots q$, то $p_{n-1}=q$, и лемма доказана; если же нет, то аналогичными рассуждениями получаем, что $(p_1p_2\cdot\ldots\cdot p_{n-2})\vdots q$ и т. д. Продолжая рассуждения, мы либо на одном из шагов получим, что $p_i\vdots q$ (а следовательно, $p_i=q$), где $2\leqslant i\leqslant n$, либо в конце концов придём к тому, что $p_1\vdots q$ (т. е. $p_1=q$). Лемма доказана.

Теорема 11 (основная теорема арифметики). Любое натуральное число, большее единицы, раскладывается в произведение простых множителей единственным (с точностью до порядка множителей) способом.

Доказательство. Существование разложения для составных чисел было доказано выше (для простых чисел существование разложения очевидно). Докажем единственность разложения.

Пусть существуют два разложения некоторого числа a на простые множители:

$$a=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_n^{\alpha_n}=p_1^{\beta_1}\cdot p_2^{\beta_2}\cdot\ldots\cdot p_n^{\beta_n}, \qquad (2)$$

где $p_1, p_2, \ldots, p_n$ — различные простые числа, входящие хотя бы в одно из двух разложений числа a; $\alpha_i, \beta_i\in\mathbb{N}_0$ $(1\leqslant i\leqslant n)$.

Докажем, что $\alpha_1=\beta_1$, $\alpha_2=\beta_2$, $\ldots$, $\alpha_n=\beta_n$. Предположим, что это не так и $\alpha_i\neq\beta_i$ для некоторого i. Без ограничения общности можно считать, что $i=1$ (этого всегда можно добиться, перенумеровав простые множители) и что $\alpha_1<\beta_1$. Тогда перепишем равенство (2) в виде:

$$p_2^{\alpha_2}\cdot p_3^{\alpha_3}\cdot\ldots\cdot p_n^{\alpha_n}=p_1^{\beta_1-\alpha_1}\cdot p_2^{\beta_2}\cdot p_3^{\beta_3}\cdot\ldots\cdot p_n^{\beta_n}.$$

Поскольку $\beta_1-\alpha_1\geqslant1$, то правая часть полученного равенства делится на p_1; тогда и левая часть делится на p_1. Следовательно, по лемме хотя бы одно из простых чисел $p_2, p_3, \ldots, p_n$, входящих в разложение левой части, совпадает с p_1 — пришли к противоречию. Значит, равенства $\alpha_1=\beta_1$, $\alpha_2=\beta_2$, $\ldots$, $\alpha_n=\beta_n$ справедливы; таким образом, два записанных разложения совпадают. Теорема доказана.

Существуют и другие доказательства основной теоремы арифметики.

Теорема 12. Пусть

$$a=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_n^{\alpha_n}, \quad b=p_1^{\beta_1}\cdot p_2^{\beta_2}\cdot\ldots\cdot p_n^{\beta_n},$$

где $p_1, p_2, \ldots, p_n$ — различные простые числа, $\alpha_i, \beta_i\in\mathbb{N}_0$ $(1\leqslant i\leqslant n)$. В этом случае $a\vdots b$ тогда и только тогда, когда $\alpha_i\geqslant\beta_i$ для любого i от 1 до n включительно.

144. Пусть $a=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_n^{\alpha_n}$, $b=q_1^{\beta_1}\cdot q_2^{\beta_2}\cdot\ldots\cdot q_m^{\beta_m}$, где $p_1, p_2, \ldots, p_n$, $q_1, q_2, \ldots, q_m$ — простые числа, $\alpha_i\in\mathbb{N}$ $(1\leqslant i\leqslant n)$, $\beta_j\in\mathbb{N}$ $(1\leqslant j\leqslant m)$. Докажите, что a и b взаимно просты тогда и только тогда, когда ни одно из чисел $p_1, p_2, \ldots, p_n$ не совпадает ни с одним из чисел $q_1, q_2, \ldots, q_m$.

145. Пусть $a, b\in\mathbb{Z}$ и НОД$(a, b)=1$. Докажите, что НОД$(a^m, b^n)=1$ для любых $m, n\in\mathbb{N}$.

Как определить, является данное натуральное число простым или составным? Доказать, что число составное, иногда можно с помощью признаков делимости или сравнений по модулю. Например, 3547821 — составное число, поскольку оно делится на 3, в чём легко убедиться при помощи признака делимости; $2^{46}+1$ является составным, поскольку $2^{46}+1=2^{4\cdot11+2}+1\equiv2^2+1\equiv0 \pmod 5$ (см. пример с остатками степеней числа 2 на стр. 11). Ещё один способ доказательства того, что число составное, заключается в его разложении на некоторые (не обязательно простые) множители, например: $9991=10000-9=100^2-3^2=(100-3)(100+3)$.

Если же вам не удалось показать, что данное число является составным, то, вероятно, это число — простое. Чтобы доказать, что число a является простым, нужно проверить, что у него нет ни одного простого делителя (кроме самого числа a). Однако не обязательно проверять все простые делители от 2 до $a-1$: следующая теорема позволяет сократить проверку.

Теорема 13. Любое составное число a имеет простой делитель p такой, что $p^2 \leqslant a$.

Доказательство. Разложим число a на простые множители, упорядочив их по возрастанию: $a=p_1p_2\cdot\ldots\cdot p_n$, где $p_1 \leqslant p_2 \leqslant \ldots \leqslant p_n$. Поскольку a — составное, то простых множителей в его разложении будет не менее двух; тогда $a=p_1p_2\cdot\ldots\cdot p_n \geqslant p_1p_2 \geqslant p_1^2$, и p_1 — искомый простой делитель числа a.

Можно предложить другое доказательство теоремы 13, используя симметрию делителей, рассмотренную в § 3. Пусть k — произвольный делитель составного числа a, отличный от 1 и от a. Тогда существует дополнительный к нему делитель n, т. е. такой, что $kn=a$. Положим для определённости, что $k \leqslant n$. Тогда $k^2 \leqslant kn = a$. Если k — простое число, то оно является искомым делителем; если же k — составное, то выберем произвольный его простой делитель k_1. Докажите самостоятельно, что k_1 является искомым простым делителем числа a.

Таким образом, для того, чтобы убедиться в том, что некоторое число a является простым, достаточно проверить, что оно не делится ни на одно простое число, не превосходящее $\sqrt{a}$. Например, для доказательства простоты числа 173 необходимо проверить, что оно не делится на 2, 3, 5, 7, 11, 13; дальнейшая проверка не требуется, поскольку следующее простое число — это 17, а $17^2 > 173$. Поскольку 173 не делится ни на одно простое число от 2 до 13, то, следовательно, 173 — простое число.

Упражнения

146. Докажите теорему 12.

147. Докажите, что если $a^n \vdots p$, где $a \in \mathbb{Z}$, p — простое, $n \in \mathbb{N}$, то и $a \vdots p$.

148. Определите, сколькими нулями оканчивается число 200!.

149. Докажите, что если $a^n \vdots b^n$, то $a \vdots b$ $(n \in \mathbb{N})$.

150. Докажите, что если целые числа a и b — взаимно простые, то и числа ab и $a+b$ — взаимно простые.

151. Известно, что $x^n = y^m$ $(x, y, m, n \in \mathbb{N}$, НОД$(m, n)=1)$. Докажите, что существует $z \in \mathbb{N}$ такое, что $x=z^m$, $y=z^n$.

152. Пусть p — простое число, $p \neq 2$. Известно, что $a \not\vdots p$, $b \not\vdots p$, $(a^2-b^2) \vdots p^n$, где $n \in \mathbb{N}$. Докажите, что либо $(a+b) \vdots p^n$, либо $(a-b) \vdots p^n$.

153. Докажите, что натуральное число, большее единицы, является n-й степенью некоторого натурального числа тогда и только тогда, когда все показатели степеней в его каноническом разложении на простые множители делятся на n.

154. Пусть a, b, $c \in \mathbb{N}$, причём $a^2=bc$ и НОД$(b, c)=1$. Докажите, что b и c — полные квадраты.

155. Найдите наименьшее натуральное число, половина которого — полный квадрат натурального числа, третья часть — куб натурального числа, четверть — пятая степень натурального числа.

156. Найдите все целочисленные решения уравнений:

а) $x^2+33=y^2$;
б) $x+y=xy$;
в) $xy+12=x-3y$;
г) $2^{x^2}\cdot 3^y = 12^x$;
д) $x^2-3xy=x-3y+2$;
е) $x^2+xy-2y^2-x+y=3$.

157. Решите в натуральных числах систему:

$$\begin{cases} x+y+z=14, \\ x+yz=19. \end{cases}$$

158. Решите в натуральных числах уравнение $n^3+4mn=145$.

159. Сумма цифр натурального числа равна 21. Докажите, что оно не является полным квадратом.

160. Может ли выполняться равенство $pm^2=n^2$ для каких-нибудь m, $n \in \mathbb{N}$ и простого p?

161. Произведение трёх простых чисел в пять раз больше их суммы. Найдите эти числа.

162. Делится ли число $\dfrac{1000!}{(500!)^2}$ на 7?

163. Натуральные числа a и b взаимно просты и имеют m и n натуральных делителей соответственно. Докажите, что число ab имеет mn натуральных делителей.

164. Определите, сколько натуральных делителей имеют следующие числа: а) 2^6; б) $3^2\cdot 5^3$; в) $3^4\cdot 7^3\cdot 11^2$; г) 10!.

165. Сколько существует натуральных чисел, меньших числа a и взаимно простых с ним, если а) $a=3^6$; б) $a=2^6\cdot 3^5$; в) $a=2^6\cdot 3\cdot 5^2\cdot 13^8$?

166. Найдите все натуральные числа, которые делятся на 12 и имеют 14 различных натуральных делителей.

167. Докажите, что если четырёхзначное число n не делится ни на одно простое число от 2 до 97, то n — простое.

168. Разложите на простые множители числа а) 2002; б) 2003; в) 2004; г) 11!; д) $2^{24}-1$.

169. Докажите, что следующие числа являются составными: а) 2^9+5^{12}; б) $2\cdot 1000^2+9\cdot 1000\cdot 1004+4\cdot 1004^2$; в) $2^{14}+3^{16}$.

§ 13. Бесконечность множества простых чисел

Теорема 14. Множество простых чисел бесконечно.

Доказательство. Предположим обратное: существует всего n различных простых чисел: $p_1, p_2, \ldots, p_n$. Рассмотрим число $P = p_1 p_2 \cdot \ldots \cdot p_n + 1$. Очевидно, P не делится на p_1: если $P \vdots p_1$, то и число $P - p_1 p_2 \cdot \ldots \cdot p_n = 1$ делится на p_1, что неверно. Аналогичным образом можно показать, что P не делится на $p_2, p_3, \ldots, p_n$. Следовательно, число P не имеет ни одного простого делителя. Однако этого не может быть, поскольку любое натуральное число, большее 1, можно разложить на простые множители (см. § 12). Полученное противоречие говорит о том, что наше предположение неверно и множество простых чисел бесконечно, что и требовалось доказать.

Приведённое доказательство принадлежит великому древнегреческому математику Евклиду.

Упражнение

170. Докажите, что существует бесконечно много простых чисел, дающих при делении на 3 остаток 2.

Указание. Предположите, что таких простых чисел лишь конечное количество: $2, p_1, p_2, \ldots, p_n$. Рассмотрите число $P = 2 \cdot 3 \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_n - 1$.

§ 14. Наименьшее общее кратное

Определение. *Наименьшим общим кратным* двух или более целых чисел $a_1, a_2, \ldots, a_n$, не равных нулю, называется наименьшее натуральное число, которое делится на все эти числа. Наименьшее общее кратное чисел $a_1, a_2, \ldots, a_n$ обозначается через НОК$(a_1, a_2, \ldots, a_n)$ *).

Примеры: НОК$(10, 22) = 110$, НОК$(28, 30) = 420$, НОК$(4, 6, 30) = 60$.

Теорема 15. Пусть $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$, $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_n^{\beta_n}$, где $p_1, p_2, \ldots, p_n$ — различные простые числа, $\alpha_i, \beta_i \in \mathbb{N}_0$ $(1 \leqslant i \leqslant n)$. Положим $\gamma_i = \min(\alpha_i, \beta_i)$, $\delta_i = \max(\alpha_i, \beta_i)$ **) $(1 \leqslant i \leqslant n)$. Тогда

$$\text{НОД}(a, b) = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \ldots \cdot p_n^{\gamma_n}, \quad \text{НОК}(a, b) = p_1^{\delta_1} \cdot p_2^{\delta_2} \cdot \ldots \cdot p_n^{\delta_n}.$$

Доказательство. По теореме 12 число $D = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \ldots \cdot p_n^{\gamma_n}$ является общим делителем чисел a и b. Представим произвольный общий делитель d чисел a и b в виде $d = p_1^{\varphi_1} \cdot p_2^{\varphi_2} \cdot \ldots \cdot p_n^{\varphi_n}$ (других простых множителей в его разложении быть не может, поскольку в этом случае он не будет делителем чисел a и b). По теореме 12 должны выполняться соотношения $\varphi_i \leqslant \alpha_i$, $\varphi_i \leqslant \beta_i$ $(1 \leqslant i \leqslant n)$, откуда $\varphi_i \leqslant \min(\alpha_i, \beta_i) = \gamma_i$; следовательно, $d \leqslant D$, что и доказывает, что D — именно наибольший общий делитель. Доказательство второго равенства аналогично. Проведите его самостоятельно.

Замечание. Теорему 15 можно обобщить на случай трёх и более чисел.

Теорема 16. Любое общее кратное двух чисел a и b делится на их наименьшее общее кратное.

Доказательство. Пусть $m = \text{НОК}(a, b)$, M — произвольное общее кратное чисел a и b. Предположим, $M \not\vdots m$. Выполним деление с остатком: $M = qm + r$, где $0 < r < m$. Поскольку $M \vdots a$, $m \vdots a$, то и $r = (M - qm) \vdots a$, аналогично $r \vdots b$. Таким образом, r также является общим кратным чисел a и b и $r < m$, что противоречит тому, что m — их наименьшее общее кратное.

Отметим, что теорему 16 можно было доказать и иначе — с помощью теорем 12 и 15.

Упражнения

171. Найдите НОД и НОК чисел а) $3^2 \cdot 5 \cdot 7$ и $3 \cdot 5^3 \cdot 11^2$; б) 280 и 300; в) 288 и 324; г) 24, 594 и 1008.

172. Докажите, что $\text{НОД}(a, b) \cdot \text{НОК}(a, b) = ab$ для любых $a, b \in \mathbb{N}$.

173. Найдите натуральные числа a и b, если известно, что $\text{НОД}(a, b) = 12$, $\text{НОК}(a, b) = 420$.

174. Известно, что $\text{НОД}(m, n) + \text{НОК}(m, n) = m + n$. Докажите, что одно из чисел m, n делится на другое $(m, n \in \mathbb{N})$.

§ 15. Уравнение Пифагора

Этот параграф посвящён поиску решений в натуральных числах *уравнения Пифагора*

$$x^2 + y^2 = z^2 \tag{3}$$

(тройка чисел (a, b, c), составляющая решение этого уравнения, называется *пифагоровой тройкой*). Известно, что если числа x, y, z удовлетворяют уравнению Пифагора, то треугольник со сторонами x, y, z существует и является прямоугольным; обратно, для любого прямоугольного треугольника с катетами x, y и гипотенузой z выполнено соотношение (3). Самое простое решение уравнения Пифагора

*) В некоторых книгах можно встретить и такое обозначение для наименьшего общего кратного: $[a_1, a_2, \ldots, a_n]$.

**) Через $\min(x_1, x_2, \ldots, x_k)$ и $\max(x_1, x_2, \ldots, x_k)$ обозначают, соответственно, наименьшее и наибольшее из чисел $x_1, x_2, \ldots, x_k$.

в натуральных числах — это (3, 4, 5) (прямоугольный треугольник с катетами 3, 4 и гипотенузой 5 называется *египетским*). Существуют и другие решения уравнения Пифагора, например: (5, 12, 13). Но как найти все его решения в натуральных числах? В этом параграфе мы получим формулы, дающие все эти решения.

Заметим, что если тройка натуральных чисел (a, b, c) является решением уравнения Пифагора, то и любая тройка вида (ka, kb, kc), где k — произвольное натуральное число, также является его решением. Обратно, если тройка (ka, kb, kc) является решением уравнения Пифагора (a, b, c, $k\in\mathbb{N}$), то и тройка (a, b, c) будет его решением. Поэтому будем в дальнейшем исследовать лишь такие решения (a, b, c), для которых НОД$(a, b, c)=1$. Такие тройки называются *примитивными*. Все остальные решения получаются из примитивных умножением a, b, c на одно и то же натуральное число.

Лемма. Пусть a, b, c — натуральные числа, составляющие решение уравнения Пифагора, причём НОД$(a, b, c)=1$. Тогда одно из чисел a и b является чётным, а другое — нечётным.

Доказательство. Заметим, что числа a и b не могут оба являться чётными, поскольку в этом случае $c^2=(a^2+b^2)\vdots 2$, откуда $c\vdots 2$, что противоречит условию НОД$(a, b, c)=1$. Так как $(2t)^2=4t^2$ и $(2t+1)^2=4t^2+4t+1=4(t^2+t)+1$, то квадрат чётного числа даёт при делении на 4 остаток 0, а квадрат нечётного числа — остаток 1. Следовательно, числа a и b не могут оба являться нечётными, так как в этом случае $c^2=a^2+b^2\equiv 1+1=2 \pmod 4$, что невозможно. Таким образом, одно из чисел a и b — чётное, а другое — нечётное, что и требовалось доказать.

Теорема 17. Пусть a, b, c — натуральные числа, составляющие решение уравнения Пифагора, причём НОД$(a, b, c)=1$ и a — нечётное число. Тогда существуют взаимно простые натуральные числа u, v разной чётности такие, что $u>v$ и

$$\begin{cases} a=u^2-v^2,\\ b=2uv,\\ c=u^2+v^2. \end{cases}$$

Доказательство. Согласно лемме, b — чётное число, поскольку a — нечётное. Число c^2 является нечётным, как сумма нечётного числа a^2 и чётного b^2. Следовательно, и c — нечётное. Перепишем равенство $a^2+b^2=c^2$ в виде $b^2=(c+a)(c-a)$. Поскольку a и c — нечётные числа, то $(c+a)\vdots 2$, $(c-a)\vdots 2$. Положим $c+a=2q$, $c-a=2r$, $b=2s$, где q, r, s — некоторые натуральные числа. Тогда равенство $b^2=(c+a)(c-a)$ запишется в виде $(2s)^2=2q\cdot 2r$, или $s^2=qr$. Числа q и r

являются взаимно простыми. В самом деле, если предположить, что q и r имеют общий простой делитель p, то и числа $q+r=\frac{c+a}{2}+\frac{c-a}{2}=c$ и $q-r=\frac{c+a}{2}-\frac{c-a}{2}=a$ также делятся на p; тогда и $b^2=(c^2-a^2)\vdots p$, откуда $b\vdots p$ (поскольку p — простое). Получаем, что числа a, b, c имеют общий простой делитель p — противоречие с условием НОД$(a, b, c)=1$. Итак, q и r — взаимно простые; тогда из равенства $s^2=qr$ по основной теореме арифметики следует, что q и r — полные квадраты (см. задачу **154**): $q=u^2$, $r=v^2$, где u, $v\in\mathbb{N}$. Имеем:

$$\begin{cases} a=q-r=u^2-v^2,\\ b=2s=2\sqrt{qr}=2uv,\\ c=q+r=u^2+v^2. \end{cases}$$

Неравенство $u>v$ очевидно: ведь $c+a>c-a$, т. е. $2q>2r$, или $q>r$, откуда $u^2>v^2$, или (поскольку u, $v\in\mathbb{N}$) $u>v$. Покажем теперь, что числа u, v взаимно простые и имеют разную чётность. Если $d=$НОД$(u, v)\neq 1$, то $a=(u^2-v^2)\vdots d$, $b=(2uv)\vdots d$, $c=(u^2+v^2)\vdots d$, т. е. НОД$(a, b, c)\neq 1$, что противоречит условию. Если же u, v имеют одинаковую чётность, то $(u-v)\vdots 2$, откуда $a=((u-v)(u+v))\vdots 2$ — противоречие с условием. Теорема доказана.

Докажем обратную теорему.

Теорема 18. Пусть u, v — взаимно простые натуральные числа разной чётности, причём $u>v$. Тогда числа $a=u^2-v^2$, $b=2uv$, $c=u^2+v^2$ составляют примитивное решение уравнения Пифагора, причём a — нечётное число.

Доказательство. Проверим сначала справедливость равенства $a^2+b^2=c^2$. Действительно,

$$a^2+b^2=(u^2-v^2)^2+(2uv)^2=u^4-2u^2v^2+v^4+4u^2v^2=$$
$$=u^4+2u^2v^2+v^4=(u^2+v^2)^2=c^2.$$

Нечётность числа a следует из того, что $a=(u-v)(u+v)$, а оба числа $u-v$ и $u+v$ нечётны (так как u, v по условию имеют разную чётность). Осталось показать, что тройка (a, b, c) является примитивной (т. е. НОД$(a, b, c)=1$). Предположим, a, b, c имеют общий простой делитель p. Заметим, что $p\neq 2$ (ведь a — нечётное); следовательно, u или v делится на p, поскольку $b=(2uv)\vdots p$ и p — простое. Положим для определённости, что $u\vdots p$; но тогда и $v^2=(u^2-a)\vdots p$, откуда $v\vdots p$. Полученный вывод противоречит взаимной простоте чисел u, v. Аналогично можно рассмотреть случай, когда $v\vdots p$. Теорема доказана.

Теоремы 17 и 18 говорят лишь о примитивных решениях уравнения Пифагора. Однако на основании этих теорем можно сделать окончательный вывод о виде общего решения.

Т е о р е м а 19. Множество натуральных решений уравнения Пифагора $a^2+b^2=c^2$ задаётся формулами

$$\begin{cases} a=k(u^2-v^2), \\ b=2kuv, \\ c=k(u^2+v^2) \end{cases} \quad \text{и} \quad \begin{cases} a=2kuv, \\ b=k(u^2-v^2), \\ c=k(u^2+v^2), \end{cases} \tag{4}$$

где k — произвольное натуральное число; u, v — произвольные взаимно простые натуральные числа разной чётности такие, что $u>v$.

Доказательство теоремы непосредственно следует из теорем 17 и 18 и того, что все решения уравнения Пифагора получаются из примитивных троек умножением a, b, c на одно и то же натуральное число (см. стр. 42).

Отметим, что при $k=1$ первая система из (4) описывает случай, когда a является нечётным числом, b — чётным. Вторая система соответствует случаю, когда, наоборот, a — чётное, b — нечётное. При $k\neq 1$ оба числа a и b могут быть чётными, например: $a=6$, $b=8$, $c=10$.

Упражнения

175. Докажите, что если тройка (a, b, c) составляет решение уравнения Пифагора, то

а) хотя бы одно из чисел a, b кратно 3;

б) хотя бы одно из чисел a, b кратно 4;

в) хотя бы одно из чисел a, b, c кратно 5.

176. Укажите длины всех сторон какого-нибудь целочисленного прямоугольного треугольника*), один из катетов которого равен а) 7; б) 18.

177. Укажите длины сторон всех целочисленных прямоугольных треугольников, у которых длина гипотенузы не превышает 30.

*) Треугольник называется целочисленным, если длины всех его сторон выражаются целыми числами.

МНОГОЧЛЕНЫ

В этом разделе строчными буквами обозначены произвольные действительные числа, если нет дополнительных условий (исключение составляют показатели степеней, которые полагаются целыми и неотрицательными).

§ 16. Основные понятия

О п р е д е л е н и е. *Многочленом* от одной переменной называется выражение

$$P(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n, \tag{1}$$

где $n\in\mathbb{N}_0$; a_0, a_1, $\ldots$, a_n — произвольные числа, называемые *коэффициентами* многочлена. Если $a_0\neq 0$, то число n называют *степенью* многочлена, коэффициент a_0 — *старшим коэффициентом* многочлена, одночлен a_0x^n — *старшим членом* многочлена. Коэффициент a_n называется *свободным членом*. Величина x является *переменной*.

В этом разделе будем считать, что коэффициенты и значения переменных всех рассматриваемых многочленов принимают произвольные действительные значения, если не будет дополнительных условий.

Степень многочлена $P(x)$ обозначается через $\deg P(x)$.

П р и м е р ы: $\deg(x^3-3x^2+2)=3$, $\deg(4x^4-2x)=4$, $\deg(-7)=0$.

Выражение (1) называется *каноническим видом многочлена*. Как правило, при записи многочленов в каноническом виде опускают слагаемые с нулевыми коэффициентами: например, вместо «$0\cdot x^6+0\cdot x^5+4x^4-3x^3+0\cdot x^2-6x+0$» пишут «$4x^4-3x^3-6x$».

Особо стоит выделить многочлен, у которого все коэффициенты равны нулю (*нулевой многочлен*). Чтобы обозначить, что многочлен $P(x)$ является нулевым, пишут: $P(x)=0$. Степень нулевого многочлена полагают равной $-\infty$. Иногда считают, что степень нулевого многочлена не определена.

О п р е д е л е н и е. Многочлен, старший коэффициент которого равен 1, называется *приведённым*.

Из школьного курса алгебры известно, как найти сумму, разность и произведение двух многочленов. Сформулируем (без доказательства) теоремы, которые показывают связь степени суммы, разности или произведения двух многочленов со степенью этих многочленов.

Т е о р е м а 20. Пусть $\deg P(x)=m$, $\deg Q(x)=n$. Тогда $\deg(P(x)\,Q(x))=m+n$.

Т е о р е м а 21. Пусть $\deg P(x)=m$, $\deg Q(x)=n$. Тогда:

1) если $m=n$, то $\deg(P(x)\pm Q(x))\leqslant m$;

2) если $m\neq n$, то $\deg(P(x)\pm Q(x))=\max(m, n)$.

П р и м е ч а н и е. Возникает естественный вопрос, как интерпретировать выражения $m+n$ и $\max(m, n)$, если степень одного или обоих многочленов равна $-\infty$. В этом случае полагают, что $-\infty+(-\infty)=-\infty$ и что $-\infty+n=-\infty$, $-\infty<n$ для любого $n\in\mathbb{Z}$.

178. Приведите пример многочленов $P(x)$ и $Q(x)$ таких, что $\deg P(x)=\deg Q(x)=4$ и а) $\deg(P(x)+Q(x))=4$; б) $\deg(P(x)+Q(x))<4$.

179. Докажите теоремы 20 и 21.

О п р е д е л е н и е. *Значением многочлена* $P(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$ в точке x_0 называется число, получающееся после подстановки x_0 в выражение для $P(x)$:

$$P(x_0)=a_0x_0^n+a_1x_0^{n-1}+\ldots+a_{n-1}x_0+a_n.$$

О п р е д е л е н и е. Многочлены $P(x)$ и $Q(x)$ называются *тождественно равными*, если они принимают равные значения при любом значении переменной x.

Тождественное равенство многочленов обозначают знаком «$\equiv$», например: $x^2+2x+1\equiv(x+1)^2$. Однако часто вместо знака «$\equiv$» пишут просто «$=$», подразумевая, тем не менее, именно тождественное равенство.

З а м е ч а н и е. Формально говоря, выражение вида $(x+1)^2$ не является многочленом (см. определение многочлена). Однако, поскольку сумма, разность и произведение многочленов приводятся к каноническому виду путём раскрытия скобок и приведения подобных слагаемых, то выражения подобного вида (т. е. выражения, полученные из многочленов канонического вида при помощи операций суммы, разности и произведения, например: $(x^3-3x^2+12)-(x^2-7x+1)$, $(x+2)(x^2-3)+(x^4+x^3+x^2+x+1)(x-1)$ и т. п.) также можно рассматривать как многочлены.

Т е о р е м а 22. Свободный член произвольного многочлена $P(x)$ равен $P(0)$; сумма коэффициентов $P(x)$ равна $P(1)$.

Доказательство теоремы осуществляется подстановками $x=0$ и $x=1$ в каноническое выражение (1).

180. Найдите сумму коэффициентов многочлена, полученного после раскрытия скобок и приведения подобных слагаемых в выражении $(x-1)^{1000}(x-2)^{2000}(x-3)^{3000}$.

Р е ш е н и е. Обозначим данное выражение через $P(x)$. По теореме 22 искомая сумма равна $P(1)=(1-1)^{1000}(1-2)^{2000}(1-3)^{3000}=0$. О т в е т: 0.

Т е о р е м а 23. Пусть $P(x)$ — многочлен с целыми коэффициентами; пусть a, $b\in\mathbb{Z}$ $(a\neq b)$. Тогда $(P(a)-P(b))\vdots(a-b)$.

Д о к а з а т е л ь с т в о. Для нулевого многочлена $P(x)$ утверждение задачи очевидно. Если же $P(x)\neq0$, то запишем этот многочлен в каноническом виде: $P(x)=c_0x^n+c_1x^{n-1}+\ldots+c_{n-1}x+c_n$. Тогда

$$\begin{aligned}P(a)-P(b)&=(c_0a^n+c_1a^{n-1}+\ldots+c_{n-1}a+c_n)-\\&-(c_0b^n+c_1b^{n-1}+\ldots+c_{n-1}b+c_n)=\\&=c_0(a^n-b^n)+c_1(a^{n-1}-b^{n-1})+\ldots+c_{n-1}(a-b).\end{aligned}$$

По задаче **44** каждая из скобок делится на $a-b$; следовательно, и всё выражение делится на $a-b$, что и требовалось доказать.

О п р е д е л е н и е. Число x_0 называется *корнем многочлена* $P(x)$, если $P(x_0)=0$.

Например, число 3 является корнем многочлена x^3-2x^2-4x+3 и не является корнем многочлена $x^5+x^4-7x^2+1$.

181. Пусть $P(x)$ — многочлен с целыми коэффициентами, и $P(5)=83$. Может ли число 1 быть корнем этого многочлена?

Р е ш е н и е. Согласно теореме 23, $(P(5)-P(1))\vdots(5-1)=4$. Если $P(1)=0$, то $P(5)-P(1)=83$, но $83\not\vdots4$ — противоречие. О т в е т: нет.

Упражнения

182. Найдите степень многочлена: а) $(x-2)(x-1)x(x+1)(x+2)$; б) $x^2-(x+1)^2-(x+2)^2+(x+3)^2$.

183. Известно, что $x+2\equiv a(x^2+x+1)+(bx+c)(x+1)$. Найдите a, b, c.

184. Найдите какой-нибудь приведённый многочлен шестой степени $P(x)$ такой, что $P(1)=1$, $P(2)=2$, $P(3)=3$, $P(4)=4$, $P(5)=5$, $P(6)=6$.

У к а з а н и е. Рассмотрите многочлен $Q(x)=P(x)-x$.

185. При любом $x\in\mathbb{Z}$ значение многочлена $P(x)$ является целым числом. Верно ли, что все коэффициенты $P(x)$ — целые числа?

186. Найдите a, если известно, что $x=1$ — корень многочлена $(x^4+2)(3x-a)+(2x+a)(3x^3-1)$.

187. Докажите, что многочлен $(x-a)(x-b)-1$, где a, $b\in\mathbb{Z}$, $a\neq b$, не имеет целочисленных корней.

188. Известно, что $P(x)$ — многочлен с целыми коэффициентами и $P(2007)=1$. Докажите, что $P(x)$ не может иметь более двух целочисленных корней.

189. Пусть $P(x)$ — многочлен с целыми коэффициентами, причём $P(0)$ и $P(1)$ — чётные числа. Докажите, что $P(n)$ — чётное число для любого $n\in\mathbb{Z}$.

Указание. Используйте теорему 22.

190. Найдите сумму коэффициентов при чётных степенях многочлена $P(x)=(2x^3+3x^2-x-2)^{100}$.

Указание. Вычислите $P(1)$ и $P(-1)$.

§ 17. Деление многочленов с остатком

Многочлены, подобно целым числам, можно не только складывать, вычитать и умножать, но и делить с остатком.

Определение. *Разделить с остатком* многочлен $P(x)$ на не являющийся нулевым многочлен $Q(x)$ — значит представить его в виде

$$P(x)=S(x)\,Q(x)+R(x),$$

где $S(x)$, $R(x)$ — некоторые многочлены и $\deg R(x)<\deg Q(x)$. Многочлен $P(x)$ называется *делимым*, $Q(x)$ — *делителем*, $S(x)$ — *частным*, $R(x)$ — *остатком*.

Деление с остатком многочлена на многочлен, не являющийся нулевым, всегда возможно; при этом частное и остаток определяются единственным образом (здесь можно усмотреть аналогию с операцией деления с остатком для целых чисел).

Если $R(x)=0$, т. е. $P(x)=S(x)\,Q(x)$, то говорят, что многочлен $P(x)$ *делится* на $Q(x)$, и обозначают это известным вам знаком: $P(x)\vdots Q(x)$. В этом случае многочлен $Q(x)$ называют *делителем* многочлена $P(x)$ (очевидно, что в этом случае и $S(x)$ является делителем многочлена $P(x)$, если только $S(x)$ не является нулевым). Если же $R(x)\neq 0$, то $P(x)$ *не делится* на $Q(x)$. Это обозначают так: $P(x)\not\vdots Q(x)$.

Деление с остатком удобно выполнять «в столбик». Рассмотрим этот алгоритм на примере.

191. Разделите с остатком многочлен $6x^4+4x^3+3x^2-2x+1$ на многочлен $2x^2+x+1$.

Решение. Запишем делимое и делитель «столбиком»:

$$\begin{array}{l|l} 6x^4+4x^3+3x^2-2x+1 & 2x^2+x+1 \\ \hline & \end{array}$$

Подберём одночлен вида ax^k так, чтобы после умножения на него старший член делителя совпал со старшим членом делимого. Очевидно, это будет $3x^2$: в самом деле, $3x^2(2x^2+x+1)=6x^4+\ldots$

Умножим делитель на $3x^2$ и вычтем его из делимого:

$$\begin{array}{l|l} 6x^4+4x^3+3x^2-2x+1 & 2x^2+x+1 \\ \cline{2-2} \underline{-\,6x^4+3x^3+3x^2} & 3x^2 \\ x^3\qquad -2x+1 & \end{array}$$

Теперь подберём одночлен вида ax^k так, чтобы после умножения на него старший член делителя совпал со старшим членом полученного многочлена x^3-2x+1. Это будет $\frac{1}{2}x$. Тогда

$$\begin{array}{l|l} 6x^4+4x^3+3x^2-2x+1 & 2x^2+x+1 \\ \cline{2-2} \underline{-\,6x^4+3x^3+3x^2} & 3x^2+\frac{1}{2}x \\ -\,x^3\qquad -2x+1 & \\ \underline{-\,x^3+\frac{1}{2}x^2+\frac{1}{2}x} & \\ -\frac{1}{2}x^2-\frac{5}{2}x+1 & \end{array}$$

Снова подберём многочлен вида ax^k описанным выше образом. Это будет $-\frac{1}{4}$; тогда

$$\begin{array}{l|l} 6x^4+4x^3+3x^2-2x+1 & 2x^2+x+1 \\ \cline{2-2} \underline{-\,6x^4+3x^3+3x^2} & 3x^2+\frac{1}{2}x-\frac{1}{4} \\ -\,x^3\qquad -2x+1 & \\ \underline{-\,x^3+\frac{1}{2}x^2+\frac{1}{2}x} & \\ -\frac{1}{2}x^2-\frac{5}{2}x+1 & \\ \underline{-\,-\frac{1}{2}x^2-\frac{1}{4}x-\frac{1}{4}} & \\ -\frac{9}{4}x+\frac{5}{4} & \end{array}$$

Степень многочлена $-\frac{9}{4}x+\frac{5}{4}$ меньше степени делителя, поэтому здесь следует остановиться. Многочлен $3x^2+\frac{1}{2}x-\frac{1}{4}$ является

частным, многочлен $-\frac{9}{4}x+\frac{5}{4}$ — остатком от деления. Ответ:

$$6x^4+4x^3+3x^2-2x+1=\left(3x^2+\frac{1}{2}x-\frac{1}{4}\right)(2x^2+x+1)+\left(-\frac{9}{4}x+\frac{5}{4}\right).$$

Замечание. Запись деления в столбик без каких бы то ни было пояснений уже является полным решением. Подробные пояснения в задаче **191** были приведены для разъяснения алгоритма.

Аналогичные действия можно провести для любых других многочленов $P(x)$ и $Q(x)\neq 0$. Это и показывает возможность деления с остатком. Докажем, что деление с остатком при $Q(x)\neq 0$ всегда можно выполнить единственным способом. Предположим, это не так, т. е. найдутся многочлены $P(x)$ и $Q(x)\neq 0$ такие, что $P(x)$ можно разделить на $Q(x)$ двумя различными способами:

$$P(x)=S_1(x)\,Q(x)+R_1(x)=S_2(x)\,Q(x)+R_2(x).$$

Тогда

$$(S_1-S_2)Q=R_2-R_1 \qquad (2)$$

(для сокращения записи опустим здесь и далее обозначение переменной x). Пусть $\deg Q=n$. Если $S_1\neq S_2$, то $\deg(S_1-S_2)\geqslant 0$; тогда (по теореме 20) $\deg((S_1-S_2)Q)=\deg(S_1-S_2)+\deg Q\geqslant\deg Q=n$. С другой стороны, по определению остатка $\deg R_1(x)<n$, $\deg R_2(x)<n$; тогда (по теореме 21) $\deg(R_2-R_1)<n$. Получили противоречие (степень правой части равенства (2) меньше n, в то время как степень левой части больше или равна n). Следовательно, предположение неверно и $S_1=S_2$; тогда из равенства (2) следует, что и $R_1=R_2$. Таким образом, разделить с остатком многочлен на многочлен, не являющийся нулевым, всегда можно единственным способом.

192. При каких значениях a многочлены $P(x)=x^4+(2a+1)x^3+(2a+2)x^2+4x+3$ и $Q(x)=x^3+2ax^2+2x+1$ имеют общий корень?

Решение. Разделим $P(x)$ на $Q(x)$ с остатком:

$$\begin{array}{r|l}
x^4+(2a+1)x^3+(2a+2)x^2+4x+3 & x^3+2ax^2+2x+1 \\
\underline{-\,x^4+\quad 2ax^3+\quad 2x^2+\ x} & \hline
\quad -x^3+\quad 2ax^2+3x+3 & x+1 \\
\quad \underline{-x^3+\quad 2ax^2+2x+1} & \\
\qquad\qquad x+2 &
\end{array}$$

Итак, $P(x)=(x+1)\,Q(x)+(x+2)$. Если многочлены $P(x)$ и $Q(x)$ имеют общий корень x_0, то $P(x_0)=Q(x_0)=0$, откуда $x_0+2=0$, т. е. $x_0=-2$. Следовательно, общим корнем многочленов $P(x)$ и $Q(x)$ может

являться только -2 (отметим, что из приведённых рассуждений вовсе не следует, что -2 непременно будет являться общим корнем этих многочленов; показано лишь, что у них не может быть других общих корней). Вычислив $P(-2)$ и $Q(-2)$, найдём возможные значения a:

$$P(-2)=16-8(2a+1)+4(2a+2)-8+3=-8a+11,$$
$$Q(-2)=-8+8a-4+1=8a-11.$$

Видим, что $P(-2)=Q(-2)=0$ только при $8a-11=0$, или $a=\frac{11}{8}$.

Ответ: $a=\frac{11}{8}$.

Упражнения

193. Разделите с остатком:
а) x^2+x+1 на $x+2$;
б) $3x^4-x^2+x+2$ на $2x^2-x-4$;
в) x^n-1 на $x-1$ ($n\in\mathbb{N}$);
г) $x^{100}+1$ на $x-1$.

Примечание. В ответ следует включить не только остаток, но и частное. Лучше всего записать ответ в стандартном виде $P(x)=S(x)\,Q(x)+R(x)$.

194. При делении многочлена $A(x)$ на многочлен $B(x)\neq 0$ получились частное $Q(x)$ и остаток $R(x)$. Найдите частное и остаток от деления $a\cdot A(x)$ на $b\cdot B(x)$, где $a\neq 0$, $b\neq 0$.

195. Определите, при каких значениях a, b, c многочлен $x^4+8x^3+6ax^2+4bx+c$ делится на многочлен $x^3+6x^2+3ax+b$.

196. Числа 1 и -2 являются корнями многочлена $P(x)$, свободный член которого равен 4. Найдите остаток от деления $P(x)$ на x^3+x^2-2x.

Указание. Используйте теорему 22.

197. Докажите, что многочлен x^3+2 не может делиться на приведённый квадратный трёхчлен с целыми коэффициентами.

§ 18. Теорема Безу

Теорема 24 (теорема Э. Безу). Остаток от деления многочлена $P(x)$ на двучлен $x-\alpha$ равен $P(\alpha)$.

Доказательство. Разделим $P(x)$ на $x-\alpha$ с остатком:

$$P(x)=(x-\alpha)\,Q(x)+R(x).$$

По определению $\deg R(x)<\deg(x-\alpha)=1$; следовательно, $R(x)$ является многочленом степени 0 или $-\infty$, т. е. числом: $R(x)=r$. Тогда $P(\alpha)=(\alpha-\alpha)\,Q(\alpha)+r=r$, что и требовалось доказать.

198. Найдите остаток от деления многочлена $P(x)=x^7-3x^5+x^4-2x^3+x+4$ на $x-1$.

Р е ш е н и е. По теореме Безу искомый остаток равен $P(1)=1-3+1-2+1+4=2$. О т в е т: 2.

С л е д с т в и е 1 и з т е о р е м ы Б е з у. Многочлен $P(x)$ делится на $x-\alpha$ тогда и только тогда, когда число α является корнем многочлена $P(x)$.

199. Докажите, что $(x^n-\alpha^n)\vdots(x-\alpha)$ при любом $n\in\mathbb{N}$.

Р е ш е н и е. По следствию 1 из теоремы Безу многочлен $P(x)$ делится на $x-\alpha$ тогда и только тогда, когда $P(\alpha)=0$. В данном случае $P(x)=x^n-\alpha^n$, и $P(\alpha)=\alpha^n-\alpha^n=0$.

С л е д с т в и е 2 и з т е о р е м ы Б е з у. Если $\alpha_1, \alpha_2, \ldots, \alpha_n$ — различные корни многочлена $P(x)$, то

$$P(x)=(x-\alpha_1)(x-\alpha_2)\cdot\ldots\cdot(x-\alpha_n)\,Q(x),$$

где $Q(x)$ — некоторый многочлен.

Д о к а з а т е л ь с т в о. Поскольку α_1 — корень многочлена $P(x)$, то $P(x)\vdots(x-\alpha_1)$, т. е. $P(x)=(x-\alpha_1)\,Q_1(x)$, где $Q_1(x)$ — некоторый многочлен. Число α_2 является корнем многочлена $Q_1(x)$, так как $P(\alpha_2)=(\alpha_2-\alpha_1)\,Q_1(\alpha_2)$, но $\alpha_2-\alpha_1\neq 0$ — следовательно, $Q_1(\alpha_2)=0$. Это значит, что $Q_1(x)\vdots(x-\alpha_2)$, т. е. $Q_1(x)=(x-\alpha_2)\,Q_2(x)$, где $Q_2(x)$ — некоторый многочлен. Тогда $P(x)=(x-\alpha_1)(x-\alpha_2)\,Q_2(x)$. Аналогично можно показать, что $Q_2(x)\vdots(x-\alpha_3)$ и что $P(x)$ можно представить в виде $P(x)=(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)\,Q_3(x)$, и т. д. В конечном итоге получим: $P(x)=(x-\alpha_1)(x-\alpha_2)\cdot\ldots\cdot(x-\alpha_n)\,Q_n(x)$, где $Q_n(x)$ — некоторый многочлен, что и требовалось доказать.

С л е д с т в и е 3 и з т е о р е м ы Б е з у. Ненулевой многочлен n-й степени не может иметь более n различных корней.

Д о к а з а т е л ь с т в о. Предположим противное: многочлен $P(x)$ степени n имеет m различных корней, причём $m>n$. Тогда

$$P(x)=(x-\alpha_1)(x-\alpha_2)\cdot\ldots\cdot(x-\alpha_m)\,Q(x), \qquad (3)$$

где $\alpha_1, \alpha_2, \ldots, \alpha_m$ — корни многочлена $P(x)$, а $Q(x)$ — некоторый многочлен, не являющийся нулевым. Степень левой части равенства (3) равна n, в то время как степень его правой части не ниже, чем m (почему?) — противоречие. Следовательно, многочлен $P(x)$ не может иметь более, чем n корней, что и требовалось доказать.

Это следствие можно сформулировать иначе.

С л е д с т в и е 3′ и з т е о р е м ы Б е з у. Если многочлен $a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$ имеет более n различных корней, то он нулевой.

Т е о р е м а 25. Многочлены $P(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$ и $Q(x)=b_0x^n+b_1x^{n-1}+\ldots+b_{n-1}x+b_n$ тождественно равны тогда и только тогда, когда $a_0=b_0$, $a_1=b_1$, $\ldots$, $a_n=b_n$.

Д о к а з а т е л ь с т в о. Д о с т а т о ч н о с т ь. Если $a_0=b_0$, $a_1=b_1$, $\ldots$, $a_n=b_n$, то для любого x_0

$$P(x_0)=a_0x_0^n+a_1x_0^{n-1}+\ldots+a_{n-1}x_0+a_n=$$
$$=b_0x_0^n+b_1x_0^{n-1}+\ldots+b_{n-1}x_0+b_n=Q(x_0).$$

Н е о б х о д и м о с т ь. Предположим, $P(x)\equiv Q(x)$. Рассмотрим многочлен

$$S(x)=P(x)-Q(x)=$$
$$=(a_0-b_0)x^n+(a_1-b_1)x^{n-1}+\ldots+(a_{n-1}-b_{n-1})x+(a_n-b_n).$$

По условию многочлены $P(x)$ и $Q(x)$ принимают равные значения при любом x, т. е. $S(x)=0$ для любого x. Тогда многочлен $S(x)$ — нулевой: предположим, что это не так. Пусть $\deg S(x)=n\geqslant 0$. Любое действительное число является корнем многочлена $S(x)$, в то время как по следствию 3 из теоремы Безу он не может иметь более n различных корней. Полученное противоречие показывает, что $S(x)$ является нулевым, а это по определению означает, что все его коэффициенты равны 0, т. е. $a_0-b_0=0$, $a_1-b_1=0$, $\ldots$, $a_n-b_n=0$, откуда и следует равенство соответствующих коэффициентов многочленов $P(x)$ и $Q(x)$, что и требовалось доказать.

200. При каких значениях a, b многочлен $P(x)=x^4+ax^3+bx^2-8x+4$ является квадратом некоторого другого многочлена?

Р е ш е н и е. Предположим, $P(x)=(Q(x))^2$, где $Q(x)$ — некоторый многочлен. Тогда $\deg P(x)=2\deg Q(x)=4$, откуда $\deg Q(x)=2$. Следовательно, $Q(x)$ имеет вид $\pm(x^2+px+q)$ (почему его старший коэффициент равен ± 1?), тогда

$$x^4+ax^3+bx^2-8x+4=(\pm(x^2+px+q))^2=(x^2+px+q)^2=$$
$$=x^4+2px^3+(p^2+2q)x^2+2pqx+q^2.$$

Многочлены $P(x)$ и $(Q(x))^2$ будут тождественно равны тогда и только тогда, когда будут равны их коэффициенты при одинаковых степенях, т. е.

$$\begin{cases} 2p=a,\\ p^2+2q=b,\\ 2pq=-8,\\ q^2=4. \end{cases}$$

Из последнего уравнения получаем $q=\pm 2$, тогда из третьего уравнения $p=\mp 2$ (знаки p и q противоположны). В случае $p=2$, $q=-2$ из первых двух уравнений находим: $a=4$, $b=0$. Если же $p=-2$, $q=2$, то $a=-4$, $b=8$. О т в е т: $a=4$, $b=0$; $a=-4$, $b=8$.

Для деления многочлена $P(x)$ на двучлен $x-\alpha$ существует специальный алгоритм, который носит название *схемы Горнера*. Проведём сначала теоретическое исследование.

Пусть $a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n=(x-\alpha)(b_0x^{n-1}+b_1x^{n-2}+\ldots+b_{n-2}x+b_{n-1})+r$. Раскрыв скобки в правой части и приравняв коэффициенты при одинаковых степенях, получим:

$$\begin{aligned}
a_0&=b_0,\\
a_1&=b_1-\alpha b_0,\\
a_2&=b_2-\alpha b_1,\\
&\ldots\ldots\ldots\\
a_{n-1}&=b_{n-1}-\alpha b_{n-2},\\
a_n&=\quad -\alpha b_{n-1}+r.
\end{aligned}$$

Перепишем эти равенства в другом виде:

$$\begin{aligned}
b_0&=a_0,\\
b_1&=a_1+\alpha b_0,\\
b_2&=a_2+\alpha b_1,\\
&\ldots\ldots\ldots\\
b_{n-1}&=a_{n-1}+\alpha b_{n-2},\\
r&=a_n+\alpha b_{n-1}.
\end{aligned}$$

Эти равенства позволяют предложить следующий алгоритм. Нарисуем табличку, состоящую из двух строк и $n+1$ столбцов. В первой строке запишем коэффициенты a_0, a_1, …, a_n; в первой ячейке второй строки запишем коэффициент b_0, равный a_0:

a_0	a_1	a_2	…	a_n
$b_0=a_0$			…	

Далее начнём заполнять ячейки второй строки, двигаясь слева направо. Каждое очередное число будет равно сумме числа, стоящего над ним, и умноженного на α числа, стоящего слева:

a_0	a_1	a_2	…	a_n
$b_0=a_0$	$b_1=a_1+\alpha b_0$	$b_2=a_2+\alpha b_1$	…	$r=a_n+\alpha b_{n-1}$

В результате в нижней строке получим коэффициенты частного b_0, b_1, …, b_{n-1} и остаток r.

201. Разделите с остатком многочлен $4x^4+13x^3+2x^2-x+7$ на двучлен $x+3$.

Р е ш е н и е. Применим схему Горнера (в данном случае $\alpha=-3$):

4	13	2	−1	7
4	1	−1	2	1

Таким образом, частное равно $4x^3+x^2-x+2$, остаток равен 1. О т в е т: $4x^4+13x^3+2x^2-x+7=(4x^3+x^2-x+2)(x+3)+1$.

Теорема Безу позволяет представить произвольный многочлен $P(x)$ в виде $(x-\alpha)Q(x)$, если известен корень α этого многочлена. Для многочленов второй, третьей и четвёртой степеней имеются формулы для нахождения корней по коэффициентам многочлена, но даже для многочленов третьей степени эти формулы имеют весьма громоздкий вид и представляют скорее теоретический, нежели практический интерес. Для многочленов же пятой и более высоких степеней таких формул и вовсе не существует, как не существует и какого-либо алгоритма, позволяющего найти все корни данного многочлена. Однако для поиска р а ц и о н а л ь н ы х корней многочленов существует простой алгоритм, позволяющий за конечное число шагов найти в с е р а ц и о н а л ь н ы е к о р н и многочлена любой степени. С таким алгоритмом мы познакомимся в следующем параграфе.

У п р а ж н е н и я

202. Найдите остаток от деления многочлена $x^{100}+x+1$ на а) $x+1$; б) $2x-1$; в) x^2+x-2.

У к а з а н и е. В пункте в) вспомните, какой вид имеет остаток от деления на многочлен второй степени.

203. При каких значениях a многочлен $2x^3-3x^2+ax-8$ при делении на $x-2$ даёт остаток, равный 6?

204. Определите, при каких значениях a многочлен $a^2x^3-8ax+8$ делится на многочлен $x-2$.

205. Докажите, что $(x^3-3abx+a^3+b^3)\vdots(x+a+b)$ при любых a, b.

206. Известно, что остаток от деления многочлена $P(x)$ на $x-1$ равен 3, а остаток от деления $P(x)$ на $x+1$ равен 1. Найдите остаток от деления $P(x)$ на x^2-1.

207. Найдите остаток от деления многочлена x^n-1 на x^2-1 ($n\in\mathbb{N}$, $n\geqslant 2$).

208. Многочлен $P(x^k)$ делится на $x-1$. Докажите, что он делится и на x^k-1.

П р и м е ч а н и е. Многочлен $P(x^k)$ — это выражение, полученное после подстановки x^k вместо x в каноническое выражение (1): $P(x^k)=a_0(x^k)^n+a_1(x^k)^{n-1}+\ldots+a_{n-1}x^k+a_n$.

209. Докажите, что $((x+1)^6-x^6-2x-1)\vdots(x(x+1)(2x+1))$.

210. Известно, что $\alpha\neq 0$. Докажите, что:

а) если n — чётное, то $(x^n-\alpha^n)\vdots(x+\alpha)$, $(x^n+\alpha^n)\not\vdots(x+\alpha)$;

б) если n — нечётное, то $(x^n-\alpha^n)\not\vdots(x+\alpha)$, $(x^n+\alpha^n)\vdots(x+\alpha)$.

211. Пусть $P(x)$ — многочлен с целыми коэффициентами. Уравнение $P(x)=1$ имеет четыре различных целых корня. Докажите, что уравнение $P(x)=-1$ не имеет целочисленных решений.

212. Упростите выражение

$$P(x)=\frac{(x-a)(x-b)(x-c)}{(d-a)(d-b)(d-c)}+\frac{(x-b)(x-c)(x-d)}{(a-b)(a-c)(a-d)}+$$
$$+\frac{(x-c)(x-d)(x-a)}{(b-c)(b-d)(b-a)}+\frac{(x-d)(x-a)(x-b)}{(c-d)(c-a)(c-b)}-1,$$

где a, b, c, d — произвольные различные числа.

Указание. Докажите, что многочлен $P(x)$ имеет по крайней мере четыре различных корня.

§ 19. Поиск рациональных корней многочлена

Теорема 26. Пусть $P(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$ — многочлен с целыми коэффициентами, $\alpha=\frac{k}{m}$ — его рациональный ненулевой корень, причём дробь $\frac{k}{m}$ несократима. Тогда $a_n\vdots k$, $a_0\vdots m$.

Доказательство. По условию

$$a_0\frac{k^n}{m^n}+a_1\frac{k^{n-1}}{m^{n-1}}+\ldots+a_{n-1}\frac{k}{m}+a_n=0.$$

Умножим обе части этого равенства на m^n и перенесём последнее слагаемое в правую часть:

$$a_0k^n+a_1k^{n-1}m+\ldots+a_{n-1}km^{n-1}=-a_nm^n.$$

Все слагаемые левой части делятся на k — следовательно, $(a_nm^n)\vdots k$. Поскольку НОД$(m, k)=1$ (из условия несократимости дроби), то и НОД$(m^n, k)=1$, и тогда (по теореме 6) $a_n\vdots k$, что и требовалось доказать. Доказательство второго утверждения аналогично. Проведите его самостоятельно.

Следствие из теоремы 26. Пусть $P(x)=x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$ — приведённый многочлен с целыми коэффициентами, α — его рациональный ненулевой корень. Тогда $\alpha\in\mathbb{Z}$ и $a_n\vdots\alpha$.

Как видно из сформулированного следствия, приведённый многочлен с целыми коэффициентами не может иметь рациональных нецелых корней.

Примечание. Подчеркнём, что теорема 26 и следствие из неё применимы лишь для поиска ненулевых корней многочленов. Очевидно, что нулевым корнем многочлен обладает тогда и только тогда, когда его свободный член равен нулю.

С использованием теоремы 26 поиск рациональных корней любого многочлена сводится к простому перебору всех возможных значений. Разберём применение этой теоремы на примере.

213. Найдите все рациональные корни многочлена $2x^4+5x^3-10x-12$.

Решение. Очевидно, $x=0$ не является корнем данного многочлена. Все ненулевые рациональные корни по теореме 26 имеют вид $\frac{k}{m}$, где НОД$(k, m)=1$, $(-12)\vdots k$, $2\vdots m$. Выпишем все возможные значения $\frac{k}{m}$:

$$\pm1,\ \pm2,\ \pm3,\ \pm4,\ \pm6,\ \pm12,\ \pm\frac{1}{2},\ \pm\frac{3}{2}.$$

Выполнив подстановку, убеждаемся, что только числа (-2) и $\frac{3}{2}$ являются корнями данного многочлена. Ответ: -2; $\frac{3}{2}$.

214. Решите уравнение $x^4+9x^3+15x^2+2x=0$.

Решение. Поскольку

$$x^4+9x^3+15x^2+2x=x(x^3+9x^2+15x+2),$$

то корнями данного уравнения будут $x=0$ и все корни многочлена $P(x)=x^3+9x^2+15x+2$. По следствию из теоремы 26 ненулевые рациональные корни многочлена $P(x)$ следует искать среди чисел ±1, ±2. Непосредственной подстановкой убеждаемся, что число -2 является корнем этого многочлена; тогда $P(x)\vdots(x+2)$ по теореме Безу. Выполнив деление, получим:

$$x^3+9x^2+15x+2=(x^2+7x+1)(x+2).$$

Решив уравнение $x^2+7x+1=0$, получим ещё два корня: $x=\frac{-7\pm\sqrt{45}}{2}$. Ответ: -2; 0; $\frac{-7\pm\sqrt{45}}{2}$.

Замечание. При решении задачи **214** можно было заметить, что если $x\geqslant 0$, то $P(x)>0$ (поскольку все коэффициенты $P(x)$ положительны); следовательно, выполняя подстановку, можно было ограничиться лишь рассмотрением отрицательных значений. Это позволило бы сократить вычислительную работу.

Упражнения

215. Найдите все рациональные корни многочленов:
а) $2x^3+x^2+5x-3$; в) x^4-x-6;
б) x^3+x+10; г) $4x^3+x-15$.

216. Решите уравнения:
а) $x^3-2x^2-6x+4=0$; в) $2x^4+7x^3+6x^2+7x-6=0$.
б) $3x^3-4x^2-7x-2=0$;

217. Докажите, что уравнение $x^p+x^{p-1}+\ldots+x^2+x+p=0$, где p — простое число, не имеет рациональных корней.

§ 20. Разложение на множители

Из школьного курса алгебры известны некоторые приёмы разложения многочленов на множители: вынесение общего множителя за скобки, группировка слагаемых, применение формул сокращённого умножения, введение дополнительных слагаемых (например, дополнение до квадрата суммы), замена переменной. В § 18 был рассмотрен ещё один способ, который даёт возможность представить многочлен в виде произведения многочленов меньшей степени, если известен один или несколько корней этого многочлена. В этом параграфе мы дадим некоторые сведения теоретического характера.

Некоторые многочлены возможно разложить на множители, представляющие собой многочлены меньших степеней: например,

$$x^3+2x^2-x-2=(x-1)(x+1)(x+2).$$

Для некоторых же многочленов (например, $x^2-6x+10$) такое разложение невозможно.

О п р е д е л е н и е. Многочлены степени 1 или выше, которые нельзя представить в виде произведения нескольких многочленов степени 1 или выше, называются *неприводимыми*; многочлены степени 1 или выше, которые можно представить в виде произведения нескольких многочленов степени 1 или выше, называются *приводимыми*.

Многочлены степеней 0 и $-\infty$ не относят ни к приводимым, ни к неприводимым.

З а м е ч а н и е. Иногда неприводимость многочлена ошибочно отождествляется с отсутствием у него корней. На самом деле имеет место следствие только в одну сторону: если многочлен неприводим, то он не имеет корней (это легко доказать при помощи следствия 1 из теоремы Безу). Обратное же утверждение неверно: так, например, многочлен x^4+4 не имеет корней, однако является приводимым.

Неприводимые многочлены — это в некотором роде аналог простых чисел. Справедлива теорема, аналогичная основной теореме арифметики.

Т е о р е м а 27. Любой приведённый многочлен степени 1 или выше раскладывается в произведение приведённых неприводимых многочленов единственным (с точностью до порядка множителей) способом.

Основная идея доказательства теоремы 27 — такая же, как у основной теоремы арифметики.

З а м е ч а н и е. В теореме 27 идёт речь только о приведённых многочленах, так как для неприведённых многочленов нарушается единственность разложения. Например,

$$8x^2-20x-12=(2x-6)(4x+2)=(x-3)(8x+4)=(4x-12)(2x+1).$$

Т е о р е м а 28. Все многочлены первой степени и многочлены второй степени с отрицательным дискриминантом являются неприводимыми на множестве действительных чисел. Все многочлены второй степени с неотрицательным дискриминантом и многочлены третьей и более высоких степеней являются приводимыми на множестве действительных чисел.

Утверждение теоремы относительно многочленов первой степени очевидно. Доказательство теоремы для многочленов второй степени мы предлагаем вам в качестве задачи для самостоятельного решения. Доказательство теоремы для многочленов третьей и более высоких степеней мы не будем рассматривать.

Упражнение

218. Докажите, что квадратный трёхчлен неприводим тогда и только тогда, когда его дискриминант отрицателен.

У к а з а н и е. Необходимо доказать два утверждения:
1) если квадратный трёхчлен неприводим, то его дискриминант отрицателен;
2) если дискриминант квадратного трёхчлена отрицателен, то этот трёхчлен неприводим.
Оба утверждения удобно доказывать методом «от противного». См. также замечание на стр. 58.

§ 21. Наибольший общий делитель

О п р е д е л е н и е. *Наибольшим общим делителем* двух многочленов $P(x)$ и $Q(x)$, хотя бы один из которых не является нулевым, называется многочлен наибольшей степени $S(x)$ такой, что $P(x)\vdots S(x)$ и $Q(x)\vdots S(x)$. Наибольший общий делитель многочленов $P(x)$ и $Q(x)$ обозначают через НОД$(P(x), Q(x))$.

Наибольший общий делитель определён неоднозначно: например, наибольшим общим делителем многочленов x^2+2x+1 и x^2-1 является и многочлен $x+1$, и многочлен $2x+2$, и многочлен $-\frac{1}{3}x-\frac{1}{3}$, и любой многочлен вида $k(x+1)$, где $k\neq 0$. Это очевидным образом следует из того, что если $P(x)\vdots Q(x)$, то $P(x)\vdots(k\cdot Q(x))$, где $k\neq 0$.

Наибольший общий делитель многочленов определён с точностью до умножения на ненулевую константу. Часто наибольший общий делитель выбирают так, чтобы его старший коэффициент был равен 1.

Искать наибольший общий делитель многочленов можно двумя основными способами: разложением на неприводимые множители и при помощи алгоритма Евклида. Сформулируем две теоремы, на которые опираются эти методы (эти теоремы похожи на соответствующие теоремы, разобранные при изучении целых чисел; похожим образом выглядят и их доказательства, поэтому мы не будем их разбирать).

Теорема 29. Пусть

$$P(x)=p\cdot(S_1(x))^{\alpha_1}\cdot(S_2(x))^{\alpha_2}\cdot\ldots\cdot(S_n(x))^{\alpha_n},$$
$$Q(x)=q\cdot(S_1(x))^{\beta_1}\cdot(S_2(x))^{\beta_2}\cdot\ldots\cdot(S_n(x))^{\beta_n},$$

где $S_1(x)$, $S_2(x)$, $\ldots$, $S_n(x)$ — различные неприводимые многочлены, α_i, $\beta_i\in\mathbb{N}_0$ $(1\leqslant i\leqslant n)$, p, $q\neq 0$. Тогда

$$\text{НОД}(P(x),\,Q(x))=k\cdot(S_1(x))^{\gamma_1}\cdot(S_2(x))^{\gamma_2}\cdot\ldots\cdot(S_n(x))^{\gamma_n},$$

где $\gamma_i=\min(\alpha_i,\,\beta_i)$ $(1\leqslant i\leqslant n)$, $k\neq 0$.

Теорема 30. Пусть $P(x)$, $Q(x)$ — многочлены, не являющиеся нулевыми, и $\deg P(x)\geqslant\deg Q(x)$. Пусть также

$$\begin{aligned}
P(x)&=S_1(x)\,Q(x)+R_1(x), && \text{где } 0\leqslant\deg R_1(x)<\deg Q(x),\\
Q(x)&=S_2(x)\,R_1(x)+R_2(x), && \text{где } 0\leqslant\deg R_2(x)<\deg R_1(x),\\
R_1(x)&=S_3(x)\,R_2(x)+R_3(x), && \text{где } 0\leqslant\deg R_3(x)<\deg R_2(x),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
R_{n-2}(x)&=S_n(x)\,R_{n-1}(x)+R_n(x), && \text{где } 0\leqslant\deg R_n(x)<\deg R_{n-1}(x),\\
R_{n-1}(x)&=S_{n+1}(x)\,R_n(x).
\end{aligned}$$

Тогда $\text{НОД}(P(x),\,Q(x))=k\cdot R_n(x)$, где $k\neq 0$.

Разберём нахождение наибольшего общего делителя на примерах.

219. Найдите $\text{НОД}(x^4-x^3-x^2+x,\,x^4-x)$.

Решение. Разложим данные многочлены на неприводимые множители:

$$x^4-x^3-x^2+x=x(x^3-x^2-x+1)=x(x-1)(x^2-1)=x(x-1)^2(x+1),$$
$$x^4-x=x(x^3-1)=x(x-1)(x^2+x+1)$$

(отметим, что многочлен x^2+x+1 является неприводимым, поскольку его дискриминант отрицателен: $D=1^2-4<0$). Тогда (по теореме 29) $\text{НОД}(x^4-x^3-x^2+x,\,x^4-x)=x(x-1)$. Ответ: $x(x-1)$.

220. Найдите $\text{НОД}(x^5+2x^4-x^3+5x^2+10x+3,\,x^3-3x^2+5x-3)$.

Решение. Применим алгоритм Евклида:

$$\begin{array}{r|l}
x^5+2x^4-x^3+5x^2+10x+3 & x^3-3x^2+5x-3\\
\cline{2-2}
x^5-3x^4+5x^3-3x^2 & x^2+5x+9\\
\cline{1-1}
5x^4-6x^3+8x^2+10x+3 & \\
5x^4-15x^3+25x^2-15x & \\
\cline{1-1}
9x^3-17x^2+25x+3 & \\
9x^3-27x^2+45x-27 & \\
\cline{1-1}
10x^2-20x+30 &
\end{array}$$

Разделив все коэффициенты многочлена $10x^2-20x+30$ на 10 (наибольший общий делитель от этого не изменится), получим многочлен x^2-2x+3. Следующий шаг алгоритма:

$$\begin{array}{r|l}
x^3-3x^2+5x-3 & x^2-2x+3\\
\cline{2-2}
x^3-2x^2+3x & x-1\\
\cline{1-1}
-x^2+2x-3 & \\
-x^2+2x-3 & \\
\cline{1-1}
0 &
\end{array}$$

Наибольший общий делитель исходных многочленов — это последний ненулевой остаток, т. е. x^2-2x+3. Ответ: x^2-2x+3.

Упражнение

221. Найдите наибольший общий делитель следующих пар многочленов:

а) $x^2(x+1)^3(x^2-x+1)$ и $x^3(x+1)^2(x^2+x+1)$;
б) $(x-1)(x+3)^2(x^2+x-2)$ и $(x+2)^4(x^2+2x-3)$;
в) x^3-3x^2+x+2 и x^3-x^2-x-2;
г) x^3-x^2-x-1 и $2x^2+x+1$;
д) x^4+3x^2+4 и $x^4+x^3+3x^2+x+2$;
е) x^m-1 и x^n-1, где m, $n\in\mathbb{N}$.

§ 22. Кратные корни

Определение. Пусть $k\in\mathbb{N}_0$. Действительное число α называется *корнем кратности k* многочлена $P(x)$, если $P(x)\vdots(x-\alpha)^k$ и $P(x)\not\vdots(x-\alpha)^{k+1}$. Корень кратности 1 называется *простым корнем*, корень кратности 2 и больше — *кратным корнем*.

Например, числа 1 и -3 являются корнями кратности 1 многочлена $x^4+6x^3+9x^2-4x-12$; число -2 является корнем кратности 2 того же многочлена. Это следует из равенства

$$x^4+6x^3+9x^2-4x-12=(x-1)(x+3)(x+2)^2.$$

222. Докажите, что $x=2$ — кратный корень многочлена $P(x)=x^4-3x^3-3x^2+16x-12$. Найдите его кратность.

Р е ш е н и е. Поскольку $P(2)=16-24-12+32-12=0$, то $P(x)\vdots(x-2)$ по следствию 1 из теоремы Безу. Выполним деление при помощи схемы Горнера:

1	-3	-3	16	-12
1	-1	-5	6	0

Таким образом, $P(x)=(x-2)\,Q(x)$, где $Q(x)=x^3-x^2-5x+6$. Поскольку $Q(2)=8-4-10+6=0$, то, следовательно, $Q(x)\vdots(x-2)$. Выполним деление:

1	-1	-5	6
1	1	-3	0

Тогда $Q(x)=(x-2)\,R(x)$, где $R(x)=x^2+x-3$. Поскольку $R(2)=4+2-3\neq0$, то $R(x)\not\vdots(x-2)$; записав равенство $P(x)=(x-2)\,Q(x)=(x-2)^2\,R(x)$, видим, что $P(x)\vdots(x-2)^2$, но $P(x)\not\vdots(x-2)^3$. Это означает, что $x=2$ является корнем кратности 2 данного многочлена. О т в е т: 2.

Рассмотрев частный случай квадратного трёхчлена, можно заметить, что он имеет один корень кратности 2 тогда и только тогда, когда дискриминант трёхчлена равен 0. При положительном дискриминанте квадратный трёхчлен имеет два простых корня, при отрицательном — не имеет действительных корней.

Несложно показать, что если многочлен $P(x)$ имеет корень α_1 кратности m_1, корень α_2 кратности m_2, ..., корень α_k кратности m_k, то

$$P(x)=(x-\alpha_1)^{m_1}(x-\alpha_2)^{m_2}\cdot\ldots\cdot(x-\alpha_k)^{m_k}\,Q(x),$$

где $Q(x)$ — некоторый многочлен. Если $P(x)$ не имеет других корней, кроме α_1, α_2, ..., α_k, то $Q(x)$ состоит из произведения квадратных трёхчленов с отрицательными дискриминантами, либо имеет нулевую степень.

Упражнения

223. Найдите кратность корня $x=1$ для многочлена $x^4-x^3-3x^2+5x-2$.

224. Найдите значения a, b, c, при которых $x=-1$ является корнем кратности 3 многочлена x^5+ax^3+bx+c.

225. Определите кратность корня $x=1$ для многочлена $nx^{n+1}-(n+1)x^n+1$, где $n\in\mathbb{N}$.

226. Многочлен $P(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$ имеет кратный ненулевой корень. Докажите, что и многочлен $S(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$ тоже имеет кратный корень.

У к а з а н и е. Докажите, что $S(x)=x^n\,P\left(\frac{1}{x}\right)$.

§ 23. Теорема Виета

Т е о р е м а 31 (т е о р е м а Ф. В и е т а). Пусть x_1, x_2 — корни квадратного трёхчлена x^2+px+q. Тогда справедливы *формулы Виета*: $x_1+x_2=-p$, $x_1x_2=q$.

Д о к а з а т е л ь с т в о. Поскольку числа x_1 и x_2 являются корнями квадратного трёхчлена, то по следствию 2 из теоремы Безу

$$x^2+px+q=(x-x_1)(x-x_2)=x^2-(x_1+x_2)x+x_1x_2.$$

Следовательно, $p=-(x_1+x_2)$, $q=x_1x_2$, что и требовалось доказать.

Справедлива *обратная теорема Виета*.

Т е о р е м а 32. Пусть для чисел x_1 и x_2 выполнены соотношения $x_1+x_2=-p$, $x_1x_2=q$. Тогда x_1 и x_2 являются корнями квадратного трёхчлена x^2+px+q.

Д о к а з а т е л ь с т в о. Обозначим данный квадратный трёхчлен через $P(x)$. Заметим, что

$$P(x)=x^2+px+q=x^2-(x_1+x_2)x+x_1x_2=(x-x_1)(x-x_2).$$

Следовательно, $P(x_1)=(x_1-x_1)(x_1-x_2)=0$, т. е. x_1 является корнем многочлена $P(x)$ (аналогично для x_2), что и требовалось доказать.

Соотношения $x_1+x_2=-p$, $x_1x_2=q$ справедливы только для приведённых многочленов. Несложно обобщить их на случай произвольного старшего коэффициента: очевидно, что корни квадратного трёхчлена ax^2+bx+c совпадают с корнями приведённого квадратного трёхчлена $x^2+\frac{b}{a}x+\frac{c}{a}$ (к которому уже можно применить доказанные теоре-

мы), а потому формулы Виета в общем виде запишутся так:

$$x_1+x_2=-\frac{b}{a}, \qquad x_1x_2=\frac{c}{a}.$$

Теорему Виета и обратную к ней можно сформулировать и для многочленов третьей и более высоких степеней.

Т е о р е м а 33. Пусть $x_1, x_2, \ldots, x_n$ — корни многочлена n-й степени $a_0x^n+a_1x^{n-1}+a_2x^{n-2}+\ldots+a_{n-1}x+a_n$. Тогда справедливы *формулы Виета*:

$$\left.\begin{aligned} x_1+x_2+\ldots+x_n&=-\frac{a_1}{a_0},\\ x_1x_2+x_1x_3+\ldots+x_{n-1}x_n&=\frac{a_2}{a_0},\\ x_1x_2x_3+x_1x_2x_4+\ldots+x_{n-2}x_{n-1}x_n&=-\frac{a_3}{a_0},\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots&\\ x_1x_2\cdot\ldots\cdot x_n&=(-1)^n\frac{a_n}{a_0} \end{aligned}\right\} \quad (4)$$

(левая часть k-го равенства представляет собой сумму всевозможных произведений, состоящих из k различных элементов из набора $\{x_1, x_2, \ldots, x_n\}$; знаки в правой части чередуются).

Теперь сформулируем обратную теорему.

Т е о р е м а 34. Пусть числа $x_1, x_2, \ldots, x_n$ удовлетворяют соотношениям (4). Тогда они являются корнями многочлена $a_0x^n+a_1x^{n-1}+a_2x^{n-2}+\ldots+a_{n-1}x+a_n$.

Идея доказательства этих двух теорем такая же, как и у прямой и обратной теоремы Виета для квадратного трёхчлена. Надо использовать тот факт, что в левой части k-го равенства стоит (с точностью до знака) коэффициент при x^{n-k}, получающийся после раскрытия скобок в выражении

$$(x-x_1)(x-x_2)\cdot\ldots\cdot(x-x_n).$$

З а м е ч а н и е. Если многочлен имеет кратные корни, то каждый корень считается в теореме Виета столько раз, какова его кратность. Например, корнями многочлена $(x-1)^3(x+2)^2(x-3)$ являются $x_1=x_2=x_3=1$, $x_4=x_5=-2$, $x_6=3$. Если количество корней с учётом их кратности меньше степени многочлена (так случается, когда разложение многочлена на множители содержит неприводимые квадратные трёхчлены), то теоремой Виета воспользоваться нельзя.

Разберём несколько задач на применение теоремы Виета.

227. Напишите приведённое квадратное уравнение, корнями которого являются числа 18 и -4.

Р е ш е н и е. Поскольку $-(18+(-4))=-14$, $18\cdot(-4)=-72$, то по обратной теореме Виета уравнение $x^2-14x-72=0$ имеет корни 18 и -4. О т в е т: $x^2-14x-72=0$.

228. Решите систему

$$\begin{cases} x+y=24,\\ xy=63. \end{cases}$$

Р е ш е н и е. По обратной теореме Виета числа x, y являются корнями квадратного уравнения $t^2-24t+63=0$ (и обратно, по прямой теореме Виета два числа, являющиеся корнями этого уравнения, удовлетворяют системе). Решая это уравнение, находим его корни: $t_1=3$, $t_2=21$. Это даёт два решения системы: $(3, 21)$ и $(21, 3)$. О т в е т: $(3, 21)$, $(21, 3)$.

Рассмотрим ещё одно полезное свойство корней квадратного уравнения, вытекающее из теоремы Виета.

Т е о р е м а 35. Пусть квадратный трёхчлен x^2+px+q имеет два корня (различных или совпадающих). Тогда:

1) оба этих корня положительны тогда и только тогда, когда $p<0$, $q>0$;

2) оба этих корня отрицательны тогда и только тогда, когда $p>0$, $q>0$.

Д о к а з а т е л ь с т в о. Докажем утверждение 1. Очевидно, если $x_1>0$, $x_2>0$, то $p=-(x_1+x_2)<0$, $q=x_1x_2>0$. Обратно, если $p<0$ и $q>0$, то, следовательно, $x_1+x_2>0$ и $x_1x_2>0$. Из неравенства $x_1x_2>0$ следует, что x_1 и x_2 одного знака (оба положительны или оба отрицательны), а из неравенства $x_1+x_2>0$ следует, что они не могут быть оба отрицательны. Следовательно, $x_1>0$ и $x_2>0$.

Доказательство утверждения 2 аналогично. Проведите его самостоятельно.

229. При каких значениях параметра p уравнение

$$x^2-2(p+1)x+9p-5=0$$

имеет два различных положительных корня?

Р е ш е н и е. Для существования двух различных корней необходимо и достаточно выполнение условия $D=(2(p+1))^2-4(9p-5)>0$, или $(p+1)^2-(9p-5)>0$, а для того, чтобы корни были положительны, необходимо и достаточно выполнение условий $-2(p+1)<0$,

$9p-5>0$. Итак,

$$\begin{cases}(p+1)^2-(9p-5)>0,\\ -2(p+1)<0,\\ 9p-5>0\end{cases}\iff\begin{cases}p^2-7p+6>0,\\ p+1>0,\\ 9p-5>0\end{cases}\iff\begin{cases}(p-1)(p-6)>0,\\ p>-1,\\ p>5/9\end{cases}\iff$$

$$\iff\begin{cases}\left[\begin{array}{l}p<1,\\ p>6;\end{array}\right.\\ p>-1,\\ p>5/9\end{cases}\iff p\in(5/9;\,1)\cup(6;\,+\infty).$$

Ответ: $p\in\left(\frac{5}{9};\,1\right)\cup(6;\,+\infty)$.

Упражнения

230. Пусть x_1, x_2 — корни уравнения $2x^2+5x-1$. Не вычисляя их, найдите:

а) $x_1x_2^2+x_1^2x_2$; в) $x_1^2+x_2^2$; д) $x_1^3+x_2^3$;

б) $\frac{x_1}{x_2}+\frac{x_2}{x_1}$; г) $\frac{1}{x_1^2}+\frac{1}{x_2^2}$; е) $\frac{x_1}{x_2^2}+\frac{x_2}{x_1^2}$.

231. Пусть x_1, x_2 — корни уравнения $2x^2-3x-6=0$. Напишите какое-нибудь квадратное уравнение, которое имеет корни

а) $-x_1$ и $-x_2$; г) $\frac{1}{x_1}$ и $\frac{1}{x_2}$;

б) x_1+3 и x_2+3; д) $x_1x_2^3$ и $x_1^3x_2$;

в) $2x_1$ и $2x_2$; е) $x_1^2+x_2^2$ и x_1x_2.

232. Пусть x_1, x_2 — корни уравнения $x^2+px+q=0$. Напишите квадратное уравнение, единственным корнем которого является число $\frac{x_1^2+x_2^2}{x_1x_2}$.

233. Сумма квадратов корней уравнения $x^2-2x+a=0$ равна 16. Найдите a.

234. Определите p, если сумма кубов корней уравнения $2x^2-8x+p=0$ равна 34.

235. Корни уравнения $x^2+px+q=0$ являются целыми числами. Найдите эти корни, если $p+q=198$.

236. Определите b, если известно, что один из корней уравнения $4x^2-15x+b=0$ является квадратом другого.

237. Найдите все такие значения a, при которых уравнение $x^2+ax+6=0$ имеет два корня, которые являются а) целыми числами; б) целыми положительными числами.

238. При каких значениях параметра a уравнение $(a-2)x^2+2(a+2)x+a+3=0$ имеет два различных положительных корня?

239. Уравнения $x^2-5x+a=0$ и $x^2-7x+3a-6=0$ имеют по два корня, и корни первого уравнения на 1 меньше корней второго уравнения. Найдите a.

240. Докажите, что не существует двух дробей, не являющихся целыми числами, у которых сумма и произведение были бы целыми числами.

Указание. Используйте следствие из теоремы 26.

241. Найдите сумму $x_1^2+x_2^2+x_3^2$, где x_1, x_2, x_3 — корни уравнения $x^3+px^2+qx+r=0$.

242. Корни многочлена $2x^3-4x+1$ равны x_1, x_2, x_3. Напишите какое-нибудь уравнение, корнями которого были бы числа

а) x_1x_2, x_1x_3, x_2x_3; б) $\frac{1}{x_1x_2}$, $\frac{1}{x_1x_3}$, $\frac{1}{x_2x_3}$.

243. Многочлен x^3+ax^2-x+b имеет три корня: x_1, x_2, x_3. Известно, что $x_1=-1$, $x_2=4$. Найдите x_3 (значения a и b неизвестны).

244. Уравнение $x^3+px+q=0$ имеет три различных корня. Докажите, что $p<0$.

245. Решите системы:

а) $\begin{cases}x+y=4,\\ x^2+y^2=26;\end{cases}$ в) $\begin{cases}x+y+z=2,\\ xy+xz+yz=-11,\\ xyz=-12;\end{cases}$

б) $\begin{cases}xy=24,\\ x^2+y^2=52;\end{cases}$ г) $\begin{cases}x+y+z=4,\\ x^2+y^2+z^2=6,\\ xyz=2.\end{cases}$

246. Докажите, что если $\frac{1}{a}+\frac{1}{b}+\frac{1}{c}=\frac{1}{a+b+c}$, то среди чисел a, b, c есть два противоположных.

Указание. Рассмотрите кубический четырёхчлен, корнями которого являются числа a, b, c.

247. Учитель написал на доске квадратный трёхчлен $x^2+10x+20$, после чего по очереди каждый из учеников увеличил или уменьшил на 1 либо коэффициент при x, либо свободный член (но не оба сразу). В результате получился квадратный трёхчлен $x^2+20x+10$. Верно ли, что в некоторый момент на доске был написан трёхчлен с целыми корнями?

248. Корни многочлена $t^2+at+b+1$ — натуральные числа. Докажите, что a^2+b^2 — составное число.

§ 24. Многочлены от нескольких переменных

О п р е д е л е н и е. *Одночленом* от переменных $x_1, x_2, \ldots, x_n$ называется выражение вида $kx_1^{\alpha_1}x_2^{\alpha_2}\cdot\ldots\cdot x_n^{\alpha_n}$, где k — произвольное число, называемое *коэффициентом*, $\alpha_i \in \mathbb{N}_0$ $(1 \leqslant i \leqslant n)$.

При записи одночленов множители, имеющие нулевые степени, обычно опускают: так, например, вместо $3x_1^7x_2^0x_3x_4^0$ пишут $3x_1^7x_3$.

О п р е д е л е н и е. *Многочленом* от переменных $x_1, x_2, \ldots, x_n$ называется сумма нескольких одночленов от этих переменных, в которой приведены подобные слагаемые (т. е. одночлены, отличающиеся только коэффициентом).

П р и м е р ы: $P(x, y, z) = x^3 - 3xy^2 + 8xyz$ — многочлен от переменных x, y, z; $Q(x_1, x_2) = x_1^6 + 2x_1x_2^2 + x_2^2 - 1$ — многочлен от переменных x_1, x_2.

Отметим, что некоторые переменные могут и не входить в запись многочлена: так, например, переменные x_1 и x_4 не входят в запись многочлена $P(x_1, x_2, x_3, x_4, x_5) = x_2x_5 + 6x_2^3x_3^2 - x_5$.

Нулевой многочлен — многочлен, в состав которого входят только одночлены с нулевыми коэффициентами.

В отличие от случая одной переменной, у многочленов от нескольких переменных не существует канонического вида. Это связано с тем, что одночлены, зависящие от многих переменных, можно упорядочивать несколькими принципиально различными способами.

Степенью одночлена $kx_1^{\alpha_1}x_2^{\alpha_2}\cdot\ldots\cdot x_n^{\alpha_n}$, где $k \neq 0$, называется число $\alpha_1 + \alpha_2 + \ldots + \alpha_n$. Если же $k = 0$, то степень такого одночлена полагается равной $-\infty$ (иногда считают, что степень такого одночлена не определена). *Степенью многочлена* называется максимальная из степеней входящих в его состав одночленов.

Подчеркнём, что при определении степени многочлена следует привести подобные слагаемые. Например, было бы ошибочно считать, что степень многочлена $x^3y^2 + xy^3 + x^3y^2 + y - 2x^3y^2$ равна 5: это вообще не многочлен, поскольку подобные слагаемые не приведены. После их приведения получается многочлен $xy^3 + y$ степени 4.

Для обозначения степени одночлена или многочлена $P(x_1, x_2, \ldots, x_n)$ используется уже известное вам обозначение $\deg P(x_1, x_2, \ldots, x_n)$. Например, $\deg(5xy^2) = 3$, $\deg(x^6 + x^2y^4 + z^6) = 6$, $\deg(x + 2xy + 3xyz + 4xyzt) = 4$, $\deg(7) = 0$, $\deg(0) = -\infty$.

Иногда при записи многочленов мы будем опускать обозначения переменных, если это не будет приводить к путанице: например, вместо $P(x_1, x_2, \ldots, x_n)$ или $P(x, y, z)$ будем писать просто P.

Для многочленов от нескольких переменных верны теоремы 20 и 21 о степени суммы и произведения многочленов (см. § 16). Определения значения многочлена и тождественного равенства многочленов можно сформулировать так же, как и для многочленов от одной переменной. Теорема о тождественном равенстве многочленов также выполняется для случая нескольких переменных. Сформулируем её, не приводя доказательства.

Т е о р е м а 36. Рассмотрим два многочлена:

$$P = a_1S_1 + a_2S_2 + \ldots\ldots + a_kS_k \quad \text{и} \quad Q = b_1S_1 + b_2S_2 + \ldots + b_kS_k,$$

где $S_1, S_2, \ldots, S_k$ — различные приведённые одночлены (т. е. имеющие вид $x_1^{\alpha_1}x_2^{\alpha_2}\cdot\ldots\cdot x_n^{\alpha_n}$). Многочлены P и Q будут тождественно равны тогда и только тогда, когда $a_1 = b_1$, $a_2 = b_2$, $\ldots$, $a_k = b_k$.

Упражнение

249. В выражении $(x+y-z)^{2007}(x-y+z)^{2007}(-x+y+z)^{2007}$ раскрыли скобки и привели подобные слагаемые. Найдите сумму коэффициентов полученного многочлена.

§ 25. Симметрические многочлены

О п р е д е л е н и е. Многочлен $P(x_1, x_2, \ldots, x_n)$ называется *симметрическим*, если он не изменяется при любой перестановке переменных $x_1, x_2, \ldots, x_n$.

Например, произведём в многочлене

$$x_1^2 + x_2^2 + x_3^2 + 2x_1x_2 + 2x_1x_3 + 2x_2x_3 - x_1x_2x_3$$

следующую перестановку: x_1 заменим на x_3, x_2 заменим на x_1, x_3 заменим на x_2 (эту перестановку можно записать так: $\begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_1 & x_2 \end{pmatrix}$; каждая переменная из верхней строки переходит в переменную, расположенную под ней). Получим многочлен

$$x_3^2 + x_1^2 + x_2^2 + 2x_3x_1 + 2x_3x_2 + 2x_1x_2 - x_3x_1x_2,$$

совпадающий с исходным. Аналогичным образом можно убедиться, что при любой перестановке переменных x_1, x_2, x_3 (всего для трёх переменных существует 6 перестановок, включая тождественную, когда все переменные остаются на месте) рассматриваемый многочлен не изменится. Следовательно, этот многочлен является симметрическим.

Отметим, что при перестановке различные переменные не могут переходить в одну и ту же: например, запись $\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_4 & x_2 & x_3 \end{pmatrix}$ не задаёт

перестановку, поскольку разные переменные x_1 и x_3 переходят в одну и ту же переменную x_2. А вот перестановки, переводящие некоторые переменные сами в себя, например, $\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_3 & x_2 & x_4 & x_1 \end{pmatrix}$, допускаются.

250. Докажите, что на n переменных существует $n!$ различных перестановок.

Несложно понять, как должен выглядеть симметрический многочлен: если, например, симметрический многочлен от трёх переменных x, y, z содержит одночлен $3x^2y$, то он должен содержать и одночлены $3x^2z$, $3y^2x$ и т. п.

Среди симметрических многочленов от n переменных выделяют n *элементарных симметрических многочленов*:

$$\begin{aligned}
&\sigma_1(x_1, x_2, \ldots, x_n) = x_1 + x_2 + \ldots + x_n,\\
&\sigma_2(x_1, x_2, \ldots, x_n) = x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n,\\
&\quad\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\sigma_n(x_1, x_2, \ldots, x_n) = x_1x_2\cdot\ldots\cdot x_n.
\end{aligned}$$

В состав многочлена σ_k входят всевозможные одночлены, представляющие собой произведение k различных переменных из набора $\{x_1, x_2, \ldots, x_n\}$. Каждое произведение взято один раз: так, например, если слагаемое $x_2x_3x_4$ вошло в состав σ_3, то слагаемые $x_2x_4x_3$, $x_3x_2x_4$ и т. п. уже не входят в него.

Посмотрев на формулы Виета для многочленов произвольной степени, можно увидеть, что в левой части этих формул стоят как раз значения элементарных симметрических многочленов $\sigma_1(x_1, x_2, \ldots, x_n)$, $\sigma_2(x_1, x_2, \ldots, x_n)$, $\ldots$, $\sigma_n(x_1, x_2, \ldots, x_n)$, принимаемые, если x_1, x_2, $\ldots$, x_n — корни данного многочлена n-й степени.

Теорема 37. Любой симметрический многочлен выражается через элементарные многочлены, причём единственным образом.

Мы не будем доказывать эту теорему, поскольку её доказательство является довольно сложным. Рассмотрим два примера, в которых требуется выразить симметрический многочлен через элементарные.

251. Выразите симметрический многочлен $P(x, y, z) = x^2 + y^2 + z^2$ через элементарные симметрические многочлены от переменных x, y, z.

Решение.

$$\begin{aligned}
x^2 + y^2 + z^2 &= x^2 + y^2 + z^2 + 2xy + 2xz + 2yz - 2xy - 2xz - 2yz =\\
&= (x + y + z)^2 - 2(xy + xz + yz) = \sigma_1^2 - 2\sigma_2.
\end{aligned}$$

Ответ: $\sigma_1^2 - 2\sigma_2$.

252. Выразите симметрический многочлен $P(x, y, z) = x^3 + y^3 + z^3$ через элементарные симметрические многочлены от переменных x, y, z.

Решение. Воспользовавшись равенством

$$(x + y + z)^3 = x^3 + y^3 + z^3 + 3(x^2y + xy^2 + x^2z + xz^2 + y^2z + yz^2) + 6xyz,$$

запишем:

$$\begin{aligned}
x^3 + y^3 + z^3 &= (x + y + z)^3 - 3(x^2y + xy^2 + x^2z + xz^2 + y^2z + yz^2) - 6xyz =\\
&= \sigma_1^3 - 3(xy(x + y) + xz(x + z) + yz(y + z)) - 6\sigma_3 =\\
&= \sigma_1^3 - 3(xy(x + y + z) + xz(x + y + z) + yz(x + y + z) - 3xyz) - 6\sigma_3 =\\
&= \sigma_1^3 - 3(x + y + z)(xy + xz + yz) + 9xyz - 6\sigma_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 9\sigma_3 - 6\sigma_3 =\\
&= \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3.
\end{aligned}$$

Ответ: $\sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$.

Упражнения

253. Выразите через элементарные симметрические многочлены:
а) $x^3 + y^3$; в) $(x + y)(x + z)(y + z)$;
б) $x^4 + y^4$; г) $x^3y + x^3z + y^3x + y^3z + z^3x + z^3y$.

254. Найдите сумму кубов корней уравнения $x^2 - 3x - 8 = 0$, не вычисляя эти корни.

255. Многочлен $f(x, y)$ является симметрическим. Докажите, что если он делится на $x - y$, то он делится и на $(x - y)^2$.

ОГЛАВЛЕНИЕ