

А. А. МАЗАНИК

ДЕЛИМОСТЬ ЧИСЕЛ И СРАВНЕНИЯ

7 и 8 КЛАССЫ

ИЗДАТЕЛЬСТВО «НАРОДНАЯ АСВЕТА»
МИНСК 1971

А. А. МАЗАНИК

ДЕЛИМОСТЬ ЧИСЕЛ И СРАВНЕНИЯ

Учебный материал
для факультативных занятий

ПОСОБИЕ ДЛЯ УЧАЩИХСЯ
7 И 8 КЛАССОВ

ИЗДАТЕЛЬСТВО «НАРОДНАЯ АСВЕТА»
МИНСК 1971

СОДЕРЖАНИЕ

От автора	3
§ 1. Делимость чисел	5
§ 2. Признаки делимости	9
§ 3. Составные и простые числа	14
§ 4. Наибольший общий делитель	20
§ 5. Алгоритм Евклида	23
§ 6. Наименьшее общее кратное	30
§ 7. Сравнения и их свойства	34
§ 8. Вычеты. Теорема Ферма	39
§ 9. Уравнения в целых числах	43
§ 10. Задачи повышенной трудности	47
Ответы и решения	53
Л и т е р а т у р а	66



Scan AAW

Мазаник А. А.

М 13 Делимость чисел и сравнения. Учебный материал для факультативных занятий. Мн., «Народная асвета», 1971.

64 с. 40 000 экз. 9 к.

В книге помещен учебный материал по теме «Дополнительные вопросы арифметики целых чисел» для факультативных занятий в VII и VIII классах.

Пособие рекомендуется учителям математики и учащимся VII и VIII классов.

ОТ АВТОРА

В данной книге изложен теоретический учебный материал и даны соответствующие упражнения для факультативных занятий по теме «Дополнительные вопросы арифметики целых чисел». Главное внимание при этом сосредоточено на раскрытии содержания понятий делимости и сравнения чисел, с которыми прямо или косвенно связаны многие проблемы теории чисел.

В процессе изучения соответствующего учебного материала вы познакомитесь с алгоритмом Евклида для отыскания наибольшего общего делителя, с теоремой о существовании сколь угодно больших простых чисел, с основной теоремой арифметики о разложении чисел на простые множители, а также с отношением сравнения чисел, являющимся обобщением понятия равенства. Подобные теоремы существования и единственности, алгоритмы и обобщения известных понятий являются примерами вопросов, которыми занимается современная математическая наука.

При изучении теоретического материала рекомендуется решать все предлагаемые в данном параграфе примеры и задачи. Если же в тексте в качестве примера приведено решение той или иной задачи, то и в этом случае попытайтесь решить ее самостоятельно, а потом сверьте свое решение с помещенным в книге.

Для повторения и закрепления целесообразно использовать упражнения, которые даны после каждого параграфа. Почти ко всем из них в конце книги приведены решения или указания.

Для тех из вас, кто пожелает более глубоко изучить вопросы делимости чисел, советуем решить все примеры и задачи повышенной трудности, помещенные в § 10. Эти упражнения можно использовать и при подготовке к математическим олимпиадам.

§ 1. ДЕЛИМОСТЬ ЧИСЕЛ

I. Когда в курсе арифметики предлагалось целое число a разделить на другое целое число b , отличное от нуля, то, в зависимости от условий задания, требовалось одно из двух:

а) либо найти такое число q , которое, будучи умножено на b , дает в точности a , т. е. $b \cdot q = a$;

б) либо найти два таких целых числа q и r , чтобы имело место равенство: $a = b \cdot q + r$, причем $0 \leq r < b$.

Деление в первом случае часто называют точным делением, а деление во втором случае — делением с остатком.

Оба эти действия совпадают, если остаток r равен нулю, и тогда говорят, что число a делится нацело на число b , причем подразумевается, что a — натуральное число или нуль, а число b — натуральное число.

Так как деление целых чисел, с учетом правила знаков, сводится к делению натуральных чисел, то подобные два действия имеют место и во множестве целых чисел.

Пусть a — любое целое число, b — натуральное (целое положительное) число. Рассмотрим числа, кратные b :

$$0; \pm b; \pm 2b; \pm 3b; \dots$$

Если эти целые кратные нанести на числовую прямую, то получим отрезки, каждый длины b , отложенные от нуля по обе стороны. Каково бы ни было целое число a , оно либо совпадет с одним из концов таких отрезков, и тогда $a = b \cdot q$, либо попадет внутрь одного из них, и тогда $a = b \cdot q + r$, где $0 < r < b$.

Например: $a = 8$, $b = 2$, значит, $q = 4$;

$a = -15$, $b = 3$, тогда $q = -5$;

$a = 27$, $b = 4$, значит, $q = 6$ и $r = 3$;

$a = -32$, $b = 5$, тогда $q = -7$ и $r = 3$.

1. а) Найдите q , если: $a = 27, b = 9$; $a = -38, b = 2$.

б) Найдите q и r , если: $a = 31, b = 5$; $a = 121, b = 13$; $a = -87, b = 5$; $a = -121, b = 13$.

2. Можно ли утверждать, что если $a = b \cdot q + m$, то m есть остаток от деления a на b ? Рассмотрите примеры: $24 = 7 \cdot 3 + 3$; $31 = 7 \cdot 3 + 10$; $20 = 7 \cdot 3 - 1$, где $b = 7$.

Напомним, что рассмотренные выше числа a, b, q и r называются соответственно делимым, делителем, частным и остатком.

Если условимся рассматривать и остаток, равный нулю, то получим:

каково бы ни было целое число a и натуральное число b , всегда найдутся такие целые числа q и r , чтобы, во-первых, имело место равенство $a = b \cdot q + r$ и во-вторых, чтобы имело место неравенство $0 \leq r < b$.

Если $r = 0$, то говорят, что b делит a , или что a делится на b . Предложение: « a делится на b » обозначают так: $a : b$ (читается: a делится на b). Число b называется делителем числа a , а число a называется кратным b .

Если остаток r не равен нулю, то говорят, что «число a не делится на число b », и это предложение обозначают так: a не $: b$.

3. Какой наименьший положительный делитель имеет число a ?

4. Какой наибольший делитель имеет число a ?

5. Докажите, что любое целое число $a \neq 0$ не может иметь более $|a|$ положительных различных делителей.

II. Таким образом, мы знаем, что целое число a делится на натуральное число $b \neq 0$ тогда и только тогда, когда существует такое третье целое число q , что $a = b \cdot q$. Теперь можно рассмотреть основные теоремы о делимости целых чисел, известные из курса арифметики.

Теорема 1. Если каждое из двух слагаемых делится на одно и то же число, то и их сумма разделится на это число¹.

Доказательство. Пусть $a : b$ и $c : b$, значит, существуют такие целые числа q_1 и q_2 , что $a = bq_1$, $c = bq_2$. Но тогда $a + c = bq_1 + bq_2 = b(q_1 + q_2)$. Сумма двух целых чисел $q_1 + q_2$ есть число целое. Обозначив его через $q = q_1 + q_2$, получим: $a + c = bq$, значит, сумма $a + c$ делится на b .

¹ Для краткости в дальнейшем будем говорить «число» вместо «целое число».

6. Докажите эту же теорему для случая трех слагаемых.

7. Если уменьшаемое и вычитаемое делятся на одно и то же число, то и их разность разделится на это число. Докажите.

8. Докажите следующие утверждения:

1) Если $a : (bc)$, то $a : b$ и $a : c$.

2) Если $a : b$, то и $-a : b$.

3) Если $a : b$ и $b : c$, то $a : c$.

4) Если $a : b$, то и $ax : b$ при любом целом x .

5) Если $a : b$ и $c : b$, то $(ax + cy) : b$ при любых целых x и y .

Докажем еще одну теорему.

Теорема 2. Если одно из слагаемых не делится, а остальные делятся на одно и то же число, то их сумма не разделится на это число.

Доказательство. Пусть $a : b$, но c не $: b$. Предположим, что их сумма $(a + c) : b$, тогда $a + c = bq$, откуда $c = bq - a$. Так как $bq : b$ и $a : b$ (по условию), то и их разность c должна делиться на b , что противоречит условию. Следовательно, сумма $a + c$ не может делиться на b .

9. Верно ли утверждение: «Если сумма двух слагаемых делится на какое-нибудь число, то и каждое слагаемое делится на это же число»? Приведите примеры, подтверждающие это.

10. Верно ли утверждение: «Если ни одно слагаемое не делится на какое-нибудь число, то и сумма не разделится на это число»? Приведите примеры, подтверждающие ваш ответ.

III. Мы видели, что каково бы ни было целое число a и натуральное число b , всегда можно найти такие целые числа q и r , что $a = bq + r$, где $0 \leq r < b$.

Докажем, что такие целые числа q (частное) и r (остаток) определяются единственным образом.

Предположим, что существуют такие q_1 и r_1 и q_2 и r_2 , что $a = bq_1 + r_1$ и $a = bq_2 + r_2$, причем $0 \leq r_1 < b$ и $0 \leq r_2 < b$. Примем, для определенности, что $r_2 \geq r_1$. Тогда имеем: $bq_1 + r_1 = bq_2 + r_2$, или $bq_1 - bq_2 = r_2 - r_1$, откуда $r_2 - r_1 = b(q_1 - q_2)$. Мы видим, что $r_2 - r_1$ делится на b , а это возможно только тогда, когда

$r_2 - r_1 = 0$, ибо $0 \leq r_2 - r_1 < b$. Получим: $b(q_1 - q_2) = 0$, но $b \neq 0$, значит, $q_1 - q_2 = 0$. Следовательно, $r_2 = r_1$ и $q_1 = q_2$.

Мы доказали, что *существует единственная пара целых чисел q и r таких, что $a = bq + r$, причем $0 \leq r < b$.*

Упражнения

11. Докажите, что если остатки от деления двух чисел a и c на число b равны между собой, то разность $a - c$ делится без остатка на b .

12. Докажите обратное утверждение: если разность двух чисел a и c делится на число b , то остатки от деления a и c на b равны между собой.

13. Верны ли утверждения: 1) Если число делится на 4, то оно делится и на 2. 2) Если число делится на 2, то оно делится и на 4.

14. Верны ли утверждения: 1) Если число не делится на 5, то оно не делится на 10. 2) Всякое число, не делящееся на 10, не делится на 5.

15. Докажите следующие утверждения:

1) Сумма двух нечетных чисел есть число четное.

2) Сумма четного и нечетного числа есть число нечетное.

3) Сумма трех последовательных целых чисел делится на 3.

4) Сумма двузначного числа и числа, написанного теми же цифрами, но в обратном порядке, делится на 11.

5) Разность между двузначным числом и числом, написанным теми же цифрами, но в обратном порядке, делится на 9.

16. Докажите, что разность между трехзначным числом и числом, написанным теми же цифрами, но в обратном порядке, делится и на 9 и на 11.

17. Ниже приведены четыре утверждения. Определите, какие из них верны, а какие неверны.

1) Если сумма двух чисел — число четное, то каждое из слагаемых — число четное.

2) Если сумма двух чисел — число четное, то их разность — число четное.

3) Если произведение двух чисел — число нечетное, то каждый из сомножителей — число нечетное.

4) Если сумма двух чисел — число нечетное, то их произведение — число четное.

18. Докажите, что: 1) Произведение двух последовательных целых чисел делится на 2. 2) Произведение трех последовательных целых чисел делится на 3.

19. Докажите, что если a число целое: то: 1) $a^2 - a$ делится на 2; 2) $a^3 - a$ делится на 3.

20. Докажите, что разность квадратов: 1) двух последовательных целых чисел есть число нечетное; 2) двух последовательных нечетных чисел делится на 8; 3) двух последовательных четных чисел делится на 4.

§ 2. ПРИЗНАКИ ДЕЛИМОСТИ

I. Из курса арифметики мы знаем признаки делимости чисел на 2, на 5, на 3 и на 9 и можем, не выполняя деления, определить, разделится ли нацело данное число на любое из указанных четырех чисел. Доказанные в предыдущем параграфе теоремы позволяют вполне строго доказать все эти признаки и вывести некоторые новые.

Пусть мы имеем $(n + 1)$ — значное число¹, записанное с помощью цифр $a_n, a_{n-1}, \dots, a_1, a_0$ в десятичной системе счисления:

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

Требуется найти условия делимости этого числа N на некоторое число p . Обозначим частные и остатки от деления 10^k на число p через q_k и r_k , где $k = 1, 2, \dots, n$.

$$10 = pq_1 + r_1;$$

$$10^2 = pq_2 + r_2;$$

$$10^3 = pq_3 + r_3;$$

$$\dots$$

$$\dots$$

$$\dots$$

$$10^n = pq_n + r_n.$$

Подставив полученные выражения для 10^k в запись числа N , получим: $N = a_n(pq_n + r_n) + a_{n-1}(pq_{n-1} + r_{n-1}) + \dots + a_2(pq_2 + r_2) + a_1(pq_1 + r_1) + a_0$.

¹ В этом параграфе рассматриваются только натуральные числа.

Преобразовав это выражение для N , найдем:

$$N = (a_n q_n + a_{n-1} q_{n-1} + \dots + a_2 q_2 + a_1 q_1) p + \\ + (a_n r_n + a_{n-1} r_{n-1} + \dots + a_2 r_2 + a_1 r_1 + a_0).$$

Обозначим второе слагаемое буквой M :

$$M = a_n r_n + a_{n-1} r_{n-1} + \dots + a_2 r_2 + a_1 r_1 + a_0,$$

тогда $N = (a_n q_n + \dots + a_1 q_1) p + M$.

Мы видим, что если число M делится на p , то и N будет делиться на p , а если M не делится на p , то и N не делится на p . Этим мы доказали следующую теорему¹:

Данное число N делится на число p тогда и только тогда, когда сумма произведений цифр числа N на остатки, полученные от деления соответствующих степеней 10 на число p , делится на это число p .

а) Пусть $p = 2$. Очевидно, что тогда $r_1 = 0$; $r_2 = 0$; \dots ; $r_n = 0$, значит, $M = a_0$; следовательно:

на 2 делятся те и только те числа, последняя цифра которых делится на 2.

б) Таким же образом получаем признак делимости чисел на 5, так как $r_1 = r_2 = \dots = r_n = 0$, значит, $M = a_0$; следовательно:

чтобы число делилось на 5, необходимо и достаточно, чтобы последняя цифра была 0 или 5.

в) Выведем признак делимости чисел на 9. Так как

$$\begin{aligned} 10 &= 9 + 1, \\ 10^2 &= 99 + 1, \\ 10^3 &= 999 + 1, \\ 10^n &= 99\dots 9 + 1, \end{aligned}$$

то очевидно, что $r_1 = 1$; $r_2 = 1$; \dots ; $r_n = 1$, значит, $M = a_n + a_{n-1} + \dots + a_1 + a_0$; следовательно:

для того чтобы число делилось на 9, необходимо и достаточно, чтобы сумма его цифр делилась на 9.

г) Подобным образом выводится и признак делимости чисел на 3. Остатки от деления степеней 10 на 3 будут: $r_1 = 1$; $r_2 = 1$; \dots ; $r_n = 1$, значит, $M = a_n + a_{n-1} + \dots + a_1 + a_0$; следовательно:

для того чтобы число делилось на 3, необходимо и достаточно, чтобы сумма его цифр делилась на 3.

¹ При делении $1 = 10^0$ на p всегда получаем остаток, равный 1.

II. Рассмотрим делимость чисел на 11. Нетрудно убедиться, что остатки от деления степеней 10 на 11 будут 10 или 1, в зависимости от того, будет ли показатель степени 10 нечетным или четным числом.

$$\begin{aligned} 10 &= 11 \cdot 0 + 10, \\ 10^2 &= 11 \cdot 9 + 1, \\ 10^3 &= 11 \cdot 90 + 10 \text{ и т. д.} \end{aligned}$$

Но $10 = 11 - 1$, поэтому удобно заменить

$$a_1 \cdot 10 = a_1(11 - 1) = a_1 \cdot 11 - a_1.$$

Поступая аналогичным образом с r_3, r_5, \dots , число M представим в виде суммы двух слагаемых, одно из которых делится на 11:

$$M = (a_1 + a_3 + a_5 + \dots) \cdot 11 + [(a_0 + a_2 + a_4 + \dots) - (a_1 + a_3 + a_5 + \dots)];$$

следовательно:

на 11 делятся те и только те числа, у которых разность сумм цифр, стоящих на четных и на нечетных местах, делится на 11.

Например, число 368312 не делится на 11, ибо разность $(3 + 8 + 1) - (6 + 3 + 2) = 1$ не делится на 11. Если взять число 271436, то у него соответствующая разность сумм цифр $(2 + 1 + 3) - (7 + 4 + 6) = -11$ делится на 11, значит, и само число делится на 11.

21. Определите, какие из следующих чисел делятся на 11:

5643; 14014; 35674; 5069812; 4192716.

III. Рассмотрим признак делимости чисел на 4. Так как 100 делится на 4, а $10 = 4 \cdot 2 + 2$, то $r_1 = 2$; $r_2 = 0$; $r_3 = 0$; \dots ; $r_n = 0$. Значит, $M = a_0 + 2a_1$; следовательно:

на 4 делятся те и только те числа, у которых сумма цифр единиц и удвоенной цифры десятков делится на 4.

Признак делимости чисел на 4 обычно формулируется в другой, более удобной для применения форме. Любое число N можно представить в виде $N = A \cdot 100 + 10a_1 + a_0$, где A — число, выраженное цифрами числа N без a_1 и a_0 . Здесь $M = 10a_1 + a_0$ есть число, выраженное двумя последними цифрами. Так как $100 = 4 \cdot 25$, можно утверждать:

на 4 делятся те и только те числа, у которых две последние цифры выражают число, делящееся на 4.

22. Определите, какие из следующих чисел делятся на 4:

326; 2348; 2405; 483568.

23. Учítывая, что 100 делится на 25 и на 50, выведите признаки делимости чисел на 25 и на 50.

IV. Рассмотренные признаки делимости чисел существенно связаны с представлением чисел именно в десятичной системе счисления. Эти признаки, вообще говоря, неприменимы при других системах счисления¹.

Например, в пятеричной системе числа, оканчивающиеся нулем, могут делиться на 2, а могут и не делиться на 2.

$15 = 30_5$ — не делится на 2;

$20 = 40_5$ — делится на 2.

Если основание системы обозначить буквой d , то любое число N можно записать в виде:

$$N = a_n d^n + a_{n-1} d^{n-1} + \dots + a_1 d + a_0.$$

Рассуждая, как и в случае десятичной системы, мы получим теорему:

Данное число N делится на число p тогда и только тогда, когда сумма произведений цифр числа N на остатки, полученные от деления соответствующих степеней основания системы счисления ($d^0 = 1, d, d^2, \dots, d^n$) на число p , делится на это число p .

Пусть $d = 4$; $p = 3$.

Все остатки от деления степеней числа 4 на 3 равны 1, значит, $M = a_n + a_{n-1} + \dots + a_2 + a_1 + a_0$. Следовательно:

в четверичной системе на 3 делятся те и только те числа, сумма цифр которых делится на 3.

Упражнения

24. Учítывая, что $1000 = 8 \cdot 125$, выведите признаки делимости чисел на 8 и на 125.

25. Вместо вопросительных знаков поставьте такие цифры, чтобы каждое из данных чисел, изображенных в десятичной системе, делилось:

¹ Если вы не знакомы с недесятичными системами счисления, то этот раздел следует опустить вместе с упражнениями № 28—36.

- 1) на 5: 483?; 34?0; 5?31;
- 2) на 9: 179?; 54?7; 5?24;
- 3) на 3: 24?; 1?6; ?22.

26. Из каждого ряда чисел одно нужно удалить: оно не обладает свойством, которое есть у остальных чисел. Какое это число?

- 1) 855; 640; 401; 365; 220;
- 2) 855; 711; 540; 366; 342;
- 3) 276; 342; 444; 524; 692.

27. Взяли 5 листов бумаги. Некоторые из них разрезали на шесть частей. Некоторые из получившихся листков снова разрезали на шесть частей. После того, как это проделали несколько раз, сосчитали число получившихся кусков. Их оказалось 54. Как показать, что при подсчете произошла ошибка?

28. Сформулируйте признаки делимости:

- 1) на 10 для чисел, записанных в десятичной системе;
- 2) на 2 для чисел, записанных в двоичной системе;
- 3) на 3 для чисел, записанных в троичной системе;
- 4) на 5 для чисел, записанных в пятеричной системе;
- 5) на любое данное число, большее единицы, для чисел, записанных в системе счисления, основанием которой является это же число.

29. Сформулируйте признак делимости на 2 для чисел, записанных в системе счисления с четным основанием (2, 4, 6, 8).

30. 1) Если рассматривать числа в восьмеричной системе, то как сформулируется признак делимости на 4? Сравните с признаком делимости на 5 в десятичной системе.

2) Сформулируйте признак делимости на 3 в шестеричной системе.

31. Сформулируйте признак делимости:

- 1) на 9 для чисел, записанных в десятичной системе;
- 2) на 2 для чисел, записанных в троичной системе;
- 3) на 6 для чисел, записанных в семеричной системе;
- 4) на 7 для чисел, записанных в восьмеричной системе;
- 5) на любое данное число для чисел, записанных в системе счисления, основание которой на 1 больше данного числа.

32. Сформулируйте признак делимости:

- 1) на 3 для чисел, записанных в десятичной системе;

- 2) на 2 для чисел, записанных в пятеричной системе;
3) на 3 для чисел, записанных в семеричной системе.

33. Определите, какие из следующих чисел являются четными (делятся на 2):

1010_2 ; 1001_2 ; 1001_3 ; 430_5 ; 213_5 ; 1100_7 ; 6541_8 ; 5604_8 .

34. Определите, какие из следующих чисел делятся на 3:

2101_3 ; 220_3 ; 312_4 ; 200_4 ; 421_7 ; 231_7 ; 483_9 ; 222_9 .

35. Определите, какие из следующих чисел делятся на 5:

324_5 ; 320_5 ; 421_6 ; 523_6 ; 125_6 ; 520_6 .

36. Определите, какие из следующих чисел делятся на 7:

331_7 ; 2010_7 ; 4640_7 ; 1637_8 ; 25_8 ; 4730_8 .

§ 3. СОСТАВНЫЕ И ПРОСТЫЕ ЧИСЛА

*1. Натуральное число называется **простым**, если оно имеет два и только два различных натуральных делителя (единицу и само число), и **составным**, если у него более двух различных натуральных делителя.*

Число 1 не принадлежит ни к простым, ни к составным числам. Всякое же натуральное число, большее единицы, является либо простым, либо составным.

Докажем несколько теорем, относящихся к простым числам.

Теорема. Всякое составное число имеет по крайней мере один простой делитель.

Доказательство. Всякое составное число должно иметь делители, большие единицы. Среди этих делителей будет наименьший, обозначим его буквой p . Этот наименьший делитель будет простым числом. Если бы он был составным числом, то имел бы некоторый делитель d , больший единицы и меньший p . Но тогда первоначальное число, делясь на p , делилось бы и на его делитель d , меньший p , чего быть не может, ибо p — наименьший делитель.

37. Докажите, что всякое натуральное число, кроме единицы, имеет по крайней мере один простой делитель.

38. Если $p \neq 1$ — наименьший из делителей составного числа N , то $p^2 \leq N$. Докажите.

39. Как следствие из предыдущего утверждения докажите, что если число $N > 1$ не делится ни на одно простое число, квадраты которых не больше, чем N , то N является простым числом.

40. Делимость на какие простые числа достаточно проверить, чтобы утверждать, что число 97 является простым числом?

Теорема. *Ряд простых чисел*

$$2, 3, 5, 7, 11, 13, \dots$$

бесконечен (то есть существуют сколь угодно большие простые числа).

Еще в древней Греции знаменитый математик Евклид (III в. до н. э.) доказал эту теорему.

Доказательство. Предположим, что простых чисел конечное число и обозначим наибольшее из них буквой p . Перемножим все эти простые числа и прибавим к полученному произведению еще 1. Получим некоторое число N .

$$N = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot \dots \cdot p + 1.$$

Это число N не может быть простым, ибо оно больше p , а по нашему предположению самое большое простое число — это p . Но оно не может быть и составным. Первое слагаемое $2 \cdot 3 \cdot 5 \cdot \dots \cdot p$ делится на любое простое число, ибо по предположению здесь перемножаются все простые числа. Значит, при делении на любое простое число всегда в остатке будет единица, то есть число N не может иметь простых делителей. А по предыдущей теореме всякое составное число имеет простой делитель.

Получили противоречие, ибо всякое число, большее единицы, либо простое, либо составное число. Следовательно, предположение, что ряд простых чисел конечен, ошибочно, значит, ряд простых чисел бесконечен¹.

41. В 1850 году П. Л. Чебышев доказал, что между любым натуральным числом, большим единицы, и числом,

¹ Наибольшее число, о котором в настоящее время известно, что оно простое — $2^{2281} - 1$.

вдвое большим его, всегда имеется хотя бы одно простое число¹.

Считая известным это утверждение Чебышева, докажете самостоятельно бесконечность ряда простых чисел.

II. Как определить, является ли данное число простым или составным? Для небольших чисел это сделать несложно, достаточно лишь найти все его делители. Например, числа 2, 3, 5, 7, 11, 13, ... — простые, а числа 4, 6, 8, 9, 10, 12, ... — составные. Но если данное число велико, то такой способ установления вида числа требует много времени.

Вместо отыскания всех делителей можно последовательно проверить, делится ли данное число на простые числа, квадрат которых не больше данного числа, что несколько упрощает работу (см. задачу № 39).

Существенные упрощения получаем при наличии таблицы простых чисел. В учебнике И. Н. Шевченко, Арифметика, V—VI классы приведена таблица всех простых чисел до 1000. В настоящее время составлены таблицы простых чисел, простирающиеся до миллионов.

Рассмотрим наиболее простой способ составления таблицы простых чисел, который называется «решетом Эратосфена» по имени выдающегося греческого астронома и математика, жившего в 276—192 гг. до нашей эры.

Пусть, например, требуется выделить все простые числа из первой сотни. Составим таблицу из ста клеточек, в которые впишем все натуральные числа от 1 до 100 (см. рис.). Вычеркиваем 1, так как единица — число не простое. Следующее число 2 — простое, его сохраняем.

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

Вычеркиваем все числа, кратные 2, кроме 2, то есть вычеркиваем все числа через одно, начиная с 4.

¹ Фактически теорема утверждает, что какое бы ни было натуральное число $n > 3$, между n и $2n - 2$ содержится хотя бы одно простое число.

Вычеркиваем теперь все числа, кратные 3, кроме 3, ибо 3 — число простое.

Первое после 3 незачеркнутое число 5; оно простое, так как не делится ни на одно меньшее его простое число. Отсчитываем от него числа по пять и каждое пятое вычеркиваем.

Подобным образом вычеркиваем и все составные числа, делящиеся на 7.

Так как следующее простое число 11, причем 11^2 больше 100, следовательно, все оставшиеся невычеркнутыми числа в первой сотне — простые.

42. Используя полученную таблицу, определите, какие из следующих чисел простые, а какие составные:

41; 57; 59; 67; 91; 97.

43. Методом «Эратосфенова решета» составьте таблицу всех простых чисел, меньших 200. Подсчитайте, сколько всего простых чисел среди чисел первой сотни и сколько среди чисел второй сотни.

III. Сформулируем теорему о разложении чисел на простые множители.

Любое число, большее единицы, или простое, или может быть представлено в виде произведения простых чисел, то есть разложено на простые множители.

Доказательство. Если число $N > 1$ простое, то утверждение доказано. Если же число N составное, то по доказанной ранее теореме оно имеет простой делитель p_1 . Тогда $N = p_1 \cdot n_1$, причем $1 < n_1 < N$, ибо $1 < p_1 < N$.

Если n_1 — число простое, то теорема доказана, если же n_1 — число составное, то оно имеет простой делитель p_2 и $n_1 = p_2 \cdot n_2$, причем $1 < n_2 < n_1$; тогда $N = p_1 \cdot p_2 \cdot n_2$.

Если n_2 — число простое, то теорема доказана; если оно составное, мы продолжаем наши рассуждения.

Так как $N > n_1$; $n_1 > n_2$; $n_2 > n_3$; ..., то наши рассуждения должны рано или поздно закончиться, ибо целых положительных чисел, меньших N , конечное число. Но закончиться данный процесс может только тогда, когда какое-нибудь $n_{k-1} = p_k$ окажется числом простым.

Полученное разложение: $N = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_k$ и будет искомым разложением числа N на простые множители. Следовательно, возможность представления числа N в виде произведения простых чисел доказана.

Можно вполне строго доказать и единственность такого разложения (см. задачу № 156).

Представление числа в виде произведения простых чисел называется каноническим разложением числа.

44. Разложите на простые множители следующие числа:

$$15; 147; 31; 12; 360; 1274.$$

Может оказаться, что в каноническом разложении числа среди простых множителей будут равные между собой, как например:

$$15525 = 3 \cdot 3 \cdot 3 \cdot 5 \cdot 5 \cdot 23.$$

Используя обозначение степени вместо произведения равных сомножителей, последнее разложение можно записать так:

$$15525 = 3^3 \cdot 5^2 \cdot 23.$$

В общем случае каноническое разложение числа N будет иметь вид:

$$N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n},$$

где p_1, p_2, \dots, p_n — различные простые числа, а $\alpha_1, \alpha_2, \dots, \alpha_n$ — натуральные числа.

45. Напишите канонические разложения следующих чисел:

$$120; 160; 600; 16800; 39600.$$

IV. С древнейших времен простые числа были предметом многочисленных исследований. Многие ученые старались отыскать закон составления простых чисел, чтобы одной или несколькими формулами можно было выразить все простые числа.

Известны попытки отыскания формул, которые хотя и не выражают всех простых чисел, но позволяют найти сколь угодно большое простое число. Например, французский математик XVII в. П. Ферма нашел, что формула $2^n + 1$ дает простые числа при значениях n , равных $2^0, 2^1, 2^2, 2^3$, ибо $2^1 + 1 = 3$; $2^2 + 1 = 5$; $2^4 + 1 = 17$; $2^8 + 1 = 257$.

Ферма высказал предположение, что формула $2^n + 1$ должна давать простые числа при всяком n , равном степени 2. Это предположение долгое время принималось

как верное утверждение. Дальнейшая проверка (а эти числа при возрастании степени 2 увеличиваются очень быстро!) подтвердила, что при $n = 2^4 = 16$ число $2^{16} + 1 = 65537$ является простым.

Впервые это утверждение было опровергнуто знаменитым математиком Л. Эйлером (XVIII в.), членом Петербургской Академии наук, который доказал, что при $n = 2^5$ формула $2^n + 1$ дает число 4294967297, делящееся на 641.

Большой интерес для ученых представляли, да и сейчас еще не утратили своего интереса, вопросы распределения простых чисел в натуральном ряду. Легко заметить, что простые числа с возрастанием натуральных чисел встречаются все реже. Например, в первой сотне натуральных чисел имеется 25 простых чисел, во второй — 21, в третьей — 16. В первой тысяче натуральных чисел 168 простых чисел, во второй тысяче — 135. Можно доказать (см. задачу № 148), что существуют сколь угодно длинные участки натурального ряда, сплошь состоящие из составных чисел.

С другой стороны, существует много пар следующих друг за другом нечетных чисел, которые оба являются простыми, например пары 3 и 5; 5 и 7; 11 и 13; 17 и 19; 29 и 31; 41 и 43. Такие пары называются парами чисел близнецов.

Ученые нашли, что до 30 миллионов имеется 152892 таких пар. Но и сегодня еще не знают, существует ли бесконечно много пар простых чисел близнецов или же есть наибольшая такая пара¹.

Важнейшие результаты о законах чередования простых чисел в натуральном ряду были получены величайшими математиками Л. Эйлером и П. Л. Чебышевым.

Упражнения

46. 1) Можно ли число 1 назвать простым числом? А составным?

2) Найти закономерность, по которой построена следующая последовательность чисел:

2; 3; 5; 7; 11; 13; 17; 19; ...

¹ Пока наибольшей известной парой близнецов являются числа 1 000 000 009 649 и 1 000 000 009 651.

47. 1) Может ли сумма двух простых чисел быть числом простым?

2) Может ли быть простым числом сумма двух простых чисел, больших 2?

48. (Шутка.) Покажите, что при всех целых значениях x числа вида $1^x + 2$ — простые.

49. Докажите, что если простое число p делится на простое число q , то $p = q$.

50. Проверьте, какие из следующих чисел простые, а какие — составные:

$$2 + 1; \quad 2 \cdot 3 + 1; \quad 2 \cdot 3 \cdot 5 + 1; \quad 2 \cdot 3 \cdot 5 \cdot 7 + 1;$$

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1; \quad 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1.$$

51. Разложите на простые множители произведение

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10.$$

(Кратко оно записывается так: $10!$ и читается «10 — факториал»)¹.

52. В какой степени простое число 2 входит в каноническое разложение числа $12!$?

53. В какой степени простое число 5 входит в каноническое разложение числа $20!$?

54. Сколькими нулями оканчивается число $20!$?

55. Сколькими нулями оканчивается число $100!$?

§ 4. НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ²

В этом параграфе помещен теоретический материал и соответствующие упражнения, рекомендуемые для тех учащихся, которые в арифметике не изучали наибольший общий делитель двух чисел. Решение упражнений № 56 — 63 из данного параграфа подготовит читателя к восприятию довольно сложного теоретического материала следующего параграфа.

56. 1) Сколько различных делителей имеет число $1 \cdot 2 \cdot 3 \cdot 5$?

2) Сколько различных делителей имеет число $2 \cdot 3 \cdot 5 \cdot 7$?

¹ При решении задач № 51 — 55 сами данные числа не вычисляются.

² В этом параграфе рассматриваются лишь натуральные числа.

3) Сколько различных делителей имеет число $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$?

57. 1) Число 90 разложите на простые множители и найдите все делители этого числа.

2) Найдите все делители числа 140.

Из решения этих примеров видим, что для нахождения делителей данного числа вначале надо разложить его на простые множители. Каждый из этих множителей будет простым делителем данного числа. Перемножая простые множители по два, по три, по четыре и так далее, получаем составные делители данного числа. Кроме того, каждое число имеет делитель 1.

58. 1) Найдите все общие делители чисел 90 и 140, используя ответ к задаче № 57.

2) В одной школе 90, а в другой 140 физкультурников. На физкультурном параде обе школы должны пройти колоннами с равным числом учащихся в каждом ряду. Какие имеются возможности построения таких колонн?

Наибольшим общим делителем данных чисел называется самый больший из их общих делителей.

Можно сказать иначе:

Наибольшим общим делителем данных чисел называется самое большое число, на которое делятся все эти числа.

Например, для чисел 12 и 8 наибольшим общим делителем будет число 4 (проверьте!), что сокращенно обозначают так: $\text{НОД}(12, 8) = 4$.

59. Найдите $\text{НОД}(90, 140)$, используя решение задачи № 58.

60. 1) Числа 18 и 30 разложите на простые множители, найдите их общие делители и запишите наибольший общий делитель.

2) Найдите $\text{НОД}(120, 420)$.

Однако такой способ нахождения наибольшего общего делителя громоздкий. Существуют другие способы, более простые, с одним из которых мы сейчас и познакомимся.

Разложим числа 120 и 420 на простые множители:

$$120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5; \quad 420 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 7.$$

Простыми общими делителями этих чисел являются простые множители, имеющиеся как в одном, так

и во втором разложении. Составные общие делители можно получить только лишь при перемножении одинаковых простых множителей.

Следовательно, общие делители можно находить, не выписывая всех делителей каждого числа. В данном конкретном случае получим следующие общие делители:

$$1; 2; 3; 5; 2 \cdot 2 = 4; 2 \cdot 3 = 6; 2 \cdot 5 = 10; 3 \cdot 5 = 15;$$

$$2 \cdot 2 \cdot 3 = 12; 2 \cdot 2 \cdot 5 = 20; 2 \cdot 3 \cdot 5 = 30; 2 \cdot 2 \cdot 3 \cdot 5 = 60.$$

Отсюда находим, что $\text{НОД}(120, 420) = 60$.

Если же нужно найти наибольший общий делитель данных чисел, то можно не находить их общих делителей. Нужно только перемножить все простые множители, имеющиеся в разложениях каждого из данных чисел.

Найдем, например, $\text{НОД}(120, 540)$. Запишем их разложения на простые множители:

$$120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5; \quad 540 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 5.$$

Сравнивая простые множители в этих разложениях, видим, что общими являются следующие простые множители: 2, 2, 3 и 5. Каждый из них будет общим делителем 120 и 540. Перемножая их по два, по три и даже все четыре, будем получать общие делители, а наибольший получим, если перемножим все четыре общие делители.

$$\text{НОД}(120, 540) = 2 \cdot 2 \cdot 3 \cdot 5 = 60.$$

Чтобы найти наибольший общий делитель данных чисел, разлагаем каждое из них на простые множители и перемножаем все общие данным числам простые множители. Полученное произведение и будет наибольшим общим делителем этих чисел.

61. Найдите наибольший общий делитель следующих чисел:

а) 18 и 12; б) 27 и 18; в) 72 и 40; г) 240 и 112.

62. Имеется 70 апельсинов, 175 орехов и 210 конфет. Какое наибольшее число одинаковых подарков для детей можно сделать из этого запаса?

Из способа нахождения наибольшего общего делителя разложением на множители видно, что любой общий делитель данных чисел является делителем НОД ,

и, наоборот, всякий делитель НОД является общим делителем данных чисел. Поэтому иногда дают несколько иное определение НОД, а именно:

НОД данных чисел называется такой их общий делитель, который делится на все общие делители этих чисел.

63. Найдите все общие делители чисел 48 и 60, предварительно найдя их наибольший общий делитель.

§ 5. АЛГОРИТМ ЕВКЛИДА

1. Возьмем произвольное натуральное число N и разложим его на простые множители. Пусть $N = p_1 \cdot p_2 \cdot \dots \cdot p_k$. Очевидно, что каждый из этих множителей будет простым делителем данного числа N .

Перемножая их по два, по три, по четыре и так далее, будем получать составные делители данного числа. Следует учитывать, что каждое число имеет делитель 1.

64. 1) Найдите все делители числа 30, разложив его предварительно на простые множители.

2) То же для числа 81.

Решая последний пример, видим, что если $N = 3^4$, то его делителями являются следующие степени числа 3:

$$1 = 3^0; \quad 3^1; \quad 3^2; \quad 3^3; \quad 3^4.$$

Аналогично, если число $N = p^k$, где p — простое число, а k — натуральное число, то каждое число вида p^α , где $0 \leq \alpha \leq k$, является делителем числа N .

Пусть $N = p^k q^s$, где p и q — простые числа, а k и s — натуральные числа. Нетрудно убедиться, что все числа вида $d = p^\alpha q^\beta$, где $0 \leq \alpha \leq k$ и $0 \leq \beta \leq s$, являются делителями числа N . Действительно,

$$N = p^k q^s = (p^\alpha p^{k-\alpha}) (q^\beta q^{s-\beta}) = (p^\alpha q^\beta) (p^{k-\alpha} q^{s-\beta});$$

так как $k - \alpha \geq 0$ и $s - \beta \geq 0$, то число $p^{k-\alpha} q^{s-\beta}$ является целым числом.

Подобным образом получаем, что если $N = p_1^{\alpha_1} \times p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n}$ — каноническое разложение числа N то каждое произведение вида $d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_n^{\beta_n}$, где $0 \leq \beta_1 \leq \alpha_1$; $0 \leq \beta_2 \leq \alpha_2$; \dots ; $0 \leq \beta_n \leq \alpha_n$, является делителем числа N .

Позже (см. задачу № 162) будет доказано, что любой делитель числа $N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n}$ можно представить

в виде $d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_n^{\beta_n}$, где $0 \leq \beta_1 \leq \alpha_1$; $0 \leq \beta_2 \leq \alpha_2$; \dots ; $0 \leq \beta_n \leq \alpha_n$.

Будем применять пока это утверждение без доказательства.

Пусть, например, требуется найти все делители числа $120 = 2^3 \cdot 3 \cdot 5$. Они имеют вид $d = 2^{\beta_1} \cdot 3^{\beta_2} \cdot 5^{\beta_3}$, где $\beta_1 = 0; 1; 2; 3$; $\beta_2 = 0; 1$; $\beta_3 = 0; 1$. Следовательно, делителями числа 120 будут следующие числа:

$$\begin{aligned} 2^0 \cdot 3^0 \cdot 5^0 &= 1; & 2^1 \cdot 3^0 \cdot 5^0 &= 2; & 2^2 \cdot 3^0 \cdot 5^0 &= 4; & 2^3 \cdot 3^0 \cdot 5^0 &= 8; \\ 2^0 \cdot 3^1 \cdot 5^0 &= 3; & 2^1 \cdot 3^1 \cdot 5^0 &= 6; & 2^2 \cdot 3^1 \cdot 5^0 &= 12; & 2^3 \cdot 3^1 \cdot 5^0 &= 24; \\ 2^0 \cdot 3^0 \cdot 5^1 &= 5; & 2^1 \cdot 3^0 \cdot 5^1 &= 10; & 2^2 \cdot 3^0 \cdot 5^1 &= 20; & 2^3 \cdot 3^0 \cdot 5^1 &= 40; \\ 2^0 \cdot 3^1 \cdot 5^1 &= 15; & 2^1 \cdot 3^1 \cdot 5^1 &= 30; & 2^2 \cdot 3^1 \cdot 5^1 &= 60; & 2^3 \cdot 3^1 \cdot 5^1 &= 120. \end{aligned}$$

65. Найдите все делители следующих чисел:

а) 8; б) 36; в) 600.

66. Не находя самих делителей, определите, сколько всего различных делителей имеют следующие числа:

а) $N = 2^3 \cdot 5^2$; б) $N = p_1^3 \cdot p_2^4$; в) $N = p_1^k \cdot p_2^n$, где p_1 и p_2 — простые числа.

II. Возьмем два произвольных натуральных числа N_1 и N_2 . Они имеют общий делитель 1. Возможны и другие общие делители этих чисел.

Наибольшим общим делителем данных чисел называется наибольшее число, на которое делятся эти числа.

Докажем его существование и единственность.

Любое натуральное число N не может иметь делителей, больших этого числа N , значит, все положительные делители числа N заключены между числами 1 и N . Следовательно, число различных делителей числа N конечно.

Но если число делителей у числа N_1 конечно, и число делителей у числа N_2 конечно, то и число общих делителей этих чисел конечно. Значит, среди этих общих делителей, число которых конечно, есть наибольший и притом один.

Наибольший общий делитель чисел N_1 и N_2 обозначают так: (N_1, N_2) , а в школьных учебниках употребляется

и такая запись: НОД (N_1, N_2). Например, НОД (6,8) = 2; НОД (24,12) = 12; НОД (8,9) = 1.

Если два числа не имеют никаких других общих делителей, кроме 1, то такие числа называются взаимно простыми. Например, числа 15 и 22 взаимно простые, ибо НОД (15,22) = 1.

Так как все делители числа $N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n}$ имеют вид $d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_n^{\beta_n}$, где $0 \leq \beta_1 \leq \alpha_1$; $0 \leq \beta_2 \leq \alpha_2$; \dots ; $0 \leq \beta_n \leq \alpha_n$, то можно найти вид общих делителей двух данных чисел.

Пусть $N_1 = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n}$ и $N_2 = q_1^{\gamma_1} \cdot q_2^{\gamma_2} \cdot \dots \cdot q_k^{\gamma_k}$, где p_i и q_i есть числа простые. Всякий общий делитель чисел N_1 и N_2 может содержать только такие простые множители, которые входят и в разложение числа N_1 и в разложение числа N_2 , причем повторяются не больше, чем соответствующие простые числа повторяются в разложениях чисел N_1 и N_2 .

Например, $N_1 = 2^3 \cdot 3^3 \cdot 7$ и $N_2 = 2 \cdot 3^5 \cdot 5^2$. В разложение любого общего делителя чисел N_1 и N_2 могут входить только простые числа 2 и 3, причем 2 в степени не выше первой, а 3 — в степени не выше третьей. Наибольший общий делитель получим, если каждый из общих простых множителей взять в наивысшей возможной для него общей степени. НОД (N_1, N_2) = $2 \cdot 3^3 = 54$.

67. Найдите наибольшие общие делители следующих пар чисел: (24,84); (120,420); (323,816).

68. 1) Докажите, что каждый делитель НОД данных чисел является общим делителем этих чисел.

2) Докажите, что всякий общий делитель данных чисел является делителем их наибольшего общего делителя.

III. Рассмотренный нами способ нахождения наибольшего общего делителя разложением на множители не всегда является рациональным, простым. Пусть, например, требуется найти НОД (464899, 232921). Вся трудность состоит в том, чтобы разложить эти числа на простые множители. Не так легко и быстро найти, что $464899 = 17 \cdot 23 \cdot 29 \cdot 41$ и $232921 = 13 \cdot 19 \cdot 23 \cdot 41$. Поэтому рассмотрим еще один способ нахождения наибольшего общего делителя двух чисел: метод последовательного деления.

Этот метод основан на двух утверждениях.

1) Если большее из двух данных чисел делится на меньшее, то наибольшим общим делителем этих двух чисел будет меньшее число.

Например, $\text{НОД}(48, 12) = 12$.

Действительно, большее число делится на меньшее и меньшее число делится само на себя, значит, меньшее число есть общий их делитель.

Меньшее число не разделится ни на какое другое число, большее его, поэтому это меньшее число есть наибольший общий делитель.

69. Найдите наибольший общий делитель чисел: 75 и 25; 252 и 42; 216 и 27.

2) Если большее из двух данных чисел не делится на меньшее, то наибольший общий делитель данных чисел равен наибольшему общему делителю двух других чисел: меньшего из данных чисел и остатка, полученного от деления большего числа на меньшее.

Например, при делении 72 на 16 получим в остатке 8, значит, $\text{НОД}(72, 16) = \text{НОД}(16, 8)$.

Доказательство. Пусть a и b — любые два натуральных числа, причем $1 < b < a$. Так как a не $\div b$, то найдутся такие целые числа q и r , что $a = bq + r$, где $0 < r < b$.

Всякий общий делитель d чисел b и r будет являться и делителем числа a , ибо если $b \div d$ и $r \div d$, то и $a \div d$, так как $a = bq + r$.

С другой стороны, возьмем произвольный общий делитель d_1 чисел a и b . Тогда $r = a - bq$ также будет делиться на этот делитель d_1 , значит, делитель d_1 является общим для r и b .

Получили, что общие делители чисел a и b и чисел b и r совпадают, но тогда совпадают и их наибольшие общие делители.

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

Следовательно, чтобы найти наибольший общий делитель двух чисел, можно большее число разделить на меньшее; если деление выполнимо, то меньшее число и есть искомый наибольший общий делитель; если же при делении получается остаток, то ищем наибольший общий делитель меньшего числа и получившегося остатка.

Так как остаток меньше делителя, то всегда получаем

новую пару чисел (меньшее число и остаток), меньших, чем исходные числа. Найдем, например, НОД(96,36).

$$96 = 2 \cdot 36 + 24;$$

значит, $\text{НОД}(96,36) = \text{НОД}(36,24)$.

Рассуждая таким же образом, для чисел 36 и 24 получим:

$$36 = 1 \cdot 24 + 12, \text{ значит, } \text{НОД}(36,24) = \text{НОД}(24,12).$$

Число 24 делится на 12, поэтому $\text{НОД}(24,12) = 12$.

Итак, $\text{НОД}(96,36) = \text{НОД}(36,24) = \text{НОД}(24,12) = 12$.

Рассмотрим общий случай. Пусть $a = bq_1 + r_1$, где $0 \leq r_1 < b$.

Если $r_1 = 0$, значит, $a : b$ и $\text{НОД}(a, b) = b$. Если же $r_1 > 0$, то по второму утверждению $\text{НОД}(a, b) = \text{НОД}(b, r_1)$.

Делим b на r_1 , пусть $b = r_1 \cdot q_2 + r_2$, где $0 \leq r_2 < r_1$. Если $r_2 = 0$, то $\text{НОД}(b, r_1) = r_1$, а значит и $\text{НОД}(a, b) = r_1$. Если же $r_2 > 0$, то вновь делим r_1 на r_2 , и так далее.

Этот процесс, каковы бы ни были числа a и b , после определенного числа повторений такого последовательного деления, обязательно закончится, ибо $b_1 > r_1 > r_2 > r_3 > \dots \geq 0$, а натуральных чисел, меньших b , конечное число. Следовательно, должны найтись такие остатки r_{n-1} и r_n , что $r_{n-1} : r_n$.

Тогда $\text{НОД}(a, b) = \text{НОД}(b, r_1) = \text{НОД}(r_1, r_2) = \dots = \text{НОД}(r_{n-1}, r_n) = r_n$.

70. 1) Найдите НОД(464899, 232921).

Решение. Покажем, как удобно располагать записи при последовательном делении.

$$\begin{array}{r}
 \begin{array}{r}
 464899 \\
 - 232921 \\
 \hline
 231978 \\
 - 231978 \\
 \hline
 0
 \end{array}
 \quad
 \begin{array}{r}
 232921 \\
 | \quad 1 \\
 \hline
 231978 \\
 | \quad 1 \\
 \hline
 943 \\
 | \quad 246 \\
 \hline
 4337 \\
 - 3772 \\
 \hline
 5658 \\
 - 5658 \\
 \hline
 0
 \end{array}
 \end{array}$$

$$\text{НОД}(464899, 232921) = 943.$$

2) Найдите НОД (270, 114).

Решение.

$$\begin{array}{r}
 270 \quad | \quad 114 \\
 \underline{-228} \quad \quad 2 \\
 \\
 114 \quad | \quad 42 \\
 \underline{-84} \quad \quad 2 \\
 \\
 42 \quad | \quad 30 \\
 \underline{-30} \quad \quad 1 \\
 \\
 30 \quad | \quad 12 \\
 \underline{-24} \quad \quad 2 \\
 \\
 12 \quad | \quad 6 \\
 \underline{-12} \quad \quad 2
 \end{array}$$

Чтобы лишний раз проследить за рассуждениями при доказательстве второго предложения, запишем все последовательные деления в виде цепочки равенств:

$$270 = 2 \cdot 114 + 42;$$

$$114 = 2 \cdot 42 + 30;$$

$$42 = 1 \cdot 30 + 12;$$

$$30 = 2 \cdot 12 + 6;$$

$$12 = 2 \cdot 6.$$

Теперь очень хорошо видно, что остатки всякий раз уменьшаются. Это же будет иметь место и для любой другой пары чисел, а поэтому такое последовательное деление всегда после нескольких шагов закончится (хотя бы делением на 1).

$$\begin{aligned}
 \text{НОД}(270, 114) &= \text{НОД}(114, 42) = \text{НОД}(42, 30) = \\
 &= \text{НОД}(30, 12) = \text{НОД}(12, 6) = 6.
 \end{aligned}$$

Чтобы найти наибольший общий делитель двух чисел, делят большее число на меньшее, меньшее на первый остаток, первый остаток на второй остаток, второй на третий и так далее, до тех пор, пока не получится в остатке нуль. Тогда последний делитель и будет наибольшим общим делителем данных чисел.

Иногда последнее предложение формулируют несколько иначе: *наибольшим общим делителем является последний, отличный от нуля, остаток.*

Рассмотренный нами процесс последовательного деления обычно называют «алгоритмом Евклида» по имени древнегреческого ученого Евклида, предложившего такой способ для отыскания общей меры двух отрезков.

Алгоритмом (или алгорифмом) в средние века называли правило, по которому выполняется то или иное арифметическое действие. Это слово происходит от имени великого узбекского математика Ал-Хорезми, который в IX веке сформулировал подобные правила.

В современной математике алгоритм — это такое предписание о выполнении в определенном порядке некоторой системы операций, позволяющее решать задачи определенного класса.

71. 1) Способом последовательного деления найдите наибольший общий делитель следующих пар чисел: 60 и 45; 56 и 42; 221 и 130; 273 и 170; 391 и 299; 15456 и 14041.

2) Способом последовательного деления найдите наибольший общий делитель чисел: а) 12, 18 и 30; б) 6, 10 и 15; в) 350, 231 и 105; г) 1260, 2310 и 1995.

Указание. Так как общий делитель любых двух чисел является делителем их наибольшего общего делителя, то наибольший общий делитель трех чисел N_1 , N_2 и N_3 либо совпадает с $d = \text{НОД}(N_1, N_2)$ (когда N_3 делится на d), либо будет делителем d . Следовательно, чтобы найти способом последовательного деления наибольший общий делитель трех или более чисел, находят наибольший общий делитель каких-нибудь двух из них, потом — наибольший общий делитель найденного делителя и какого-нибудь третьего данного числа, затем — наибольший общий делитель последнего делителя и четвертого данного числа и так далее.

Упражнения

72. Найдите двумя способами (разложением на множители и последовательным делением) наибольший общий делитель чисел:

28 и 21; 80 и 64; 2688 и 512.

Сравните оба способа.

73. 1) Туристы проехали на велосипедах в первый день 56 км, а во второй — 72 км, причем каждый день были в пути целое число часов. Найдите скорость движе-

ния, если известно, что она выражалась целым числом километров в час, была все время одинакова и наибольшей из возможных.

2) Туристы прошли в первый день 36 км, во второй — 32 км и в третий — 24 км, причем каждый день были в пути целое число часов. Сколько часов они были в пути, если их скорость выражалась целым числом километров в час, была постоянной и наибольшей из возможных?

74. В одном скором поезде 432 пассажирских места, во втором — 576 и в третьем — 480. Сколько вагонов имеет каждый поезд, если известно, что в каждом вагоне одинаковое число пассажирских мест, наибольшее из возможных?

§ 6. НАИМЕНЬШЕЕ ОБЩЕЕ КРАТНОЕ

I. Возьмем два натуральных числа a и b . *Всякое число, делящееся на a и делящееся на b , называется общим кратным чисел a и b .* Очевидно, что число 0 делится на любые числа a и b . Но мы будем рассматривать лишь положительные общие кратные.

Наименьшим общим кратным данных чисел называется наименьшее натуральное число, делящееся на каждое из этих чисел.

Установим его существование и единственность.

Очевидно, что произведение $a \cdot b$ является общим кратным чисел a и b . Возможны и меньшие, чем $a \cdot b$ натуральные числа, делящиеся как на a , так и на b .

Натуральных чисел, не больших, чем $a \cdot b$, конечное число, значит, можно проверить, которые из них кратны и a и b , и выбрать среди этих нескольких общих кратных наименьшее. Следовательно, наименьшее общее кратное любых двух натуральных чисел существует и притом одно.

Заметим, что общих кратных a и b бесконечное множество, ибо всякое число вида $q \cdot (ab)$ является общим кратным a и b , каким бы ни было натуральное число q .

Наименьшее общее кратное чисел a и b обозначается $[a, b]$; в школьной математике обычно употребляется обозначение НОК(a, b). Например, НОК(15, 20) = 60; НОК(8, 9) = 72.

II. Понятие общего кратного двух чисел связано с понятием их общего делителя. Докажем следующие две теоремы.

1) Если d — общий делитель чисел a и b , то произведение $a \cdot b$ делится на d . Частное $\frac{ab}{d}$ является кратным a и b .

Доказательство. Так как $a : d$ и $b : d$, то $a = d \cdot q_1$ и $b = d \cdot q_2$. Поэтому $a \cdot b = (dq_1) \cdot (dq_2) = d(dq_1q_2)$. Мы видим, что $ab : d$, причем частное $\frac{ab}{d} = dq_1q_2$. Оно делится на a и на b , ибо $\frac{ab}{d} = (dq_1)q_2 = aq_2$ и $\frac{ab}{d} = (dq_2)q_1 = bq_1$.

Следовательно, каждому общему делителю чисел a и b соответствует общее кратное этих чисел, не большее, чем $a \cdot b$.

2) Если $m = \text{НОК}(a, b)$, то $ab : m$, причем частное $\frac{ab}{m}$ является общим делителем a и b .

Доказательство. Пусть $ab = mq + r$, где $0 \leq r < m$. Поскольку ab делится и на a и на b , и m делится как на a , так и на b , то $r = ab - mq$ должно делиться и на a и на b , то есть r есть общее кратное чисел a и b . Но m — наименьшее из положительных общих кратных a и b , следовательно, $r = 0$.

Обозначим частное $\frac{ab}{m}$ через d , тогда $\frac{ab}{m} = d$, или $ab = md$. Докажем, что $a : d$ и $b : d$.

Равенство $ab = md$ можно записать так: $\frac{m}{a} = \frac{b}{d}$ или $\frac{m}{b} = \frac{a}{d}$. Но $\frac{m}{a}$ и $\frac{m}{b}$ есть числа целые, так как $m = \text{НОК}(a, b)$, то и $\frac{b}{d}$ и $\frac{a}{d}$ — числа целые. Значит, $b : d$ и $a : d$, то есть d — есть общий делитель чисел a и b .

75. Докажите, что если $D = \text{НОД}(a, b)$, то $\frac{ab}{D} = m$, где $m = \text{НОК}(a, b)$.

Решив эту задачу, мы можем записать равенство:

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

III. На уроках арифметики вы изучали отыскание наименьшего общего кратного разложением данных чисел на простые множители. Поэтому мы не будем еще раз

рассматривать эти вопросы, а ознакомимся с еще одним способом отыскания наименьшего общего кратного.

Иногда очень трудно найти разложение данных чисел на простые множители, так как требуется производить много пробных делений, часть из которых иногда выполняется письменно. Полученная выше формула

$$a \cdot b = \text{НОД}(a, b) \cdot \text{НОК}(a, b)$$

позволяет находить НОК двух чисел без обязательного разложения данных чисел на простые множители:

$$\text{НОК}(a, b) = \frac{a \cdot b}{\text{НОД}(a, b)}.$$

НОД можно найти, например, алгоритмом Евклида, а тогда легко найти и их наименьшее общее кратное.

Наименьшее общее кратное двух чисел равно произведению этих чисел, деленному на их наибольший общий делитель.

76. Найти НОК(2261, 1729).

Решение. Методом последовательного деления найдем, что $\text{НОД}(2261, 1729) = 133$.

$$\begin{array}{r} 2261 \quad | \quad 1729 \\ - 1729 \quad | \quad 1 \\ \hline 1729 \quad | \quad 532 \\ - 1596 \quad | \quad 3 \\ \hline 532 \quad | \quad 133 \\ - 532 \quad | \quad 4 \\ \hline \end{array}$$

Находим, что $2261 \cdot 1729 = 3909269$, значит, $\text{НОК}(2261, 1729) = 3909269 : 133 = 29393$.

Примечание. Вычисления можно производить и в иной последовательности: одно из данных чисел делим на наибольший общий делитель и полученное частное умножаем на другое данное число. При таком вычислении операции производятся над меньшими числами.

$$\begin{aligned} \text{НОК}(2261, 1729) &= (2261 \cdot 1729) : 133 = 2261 \cdot (1729 : 133) = \\ &= 2261 \cdot 13 = 29393. \end{aligned}$$

Упражнения

77. Докажите, что НОК двух взаимно простых чисел равно их произведению.

78. Найдите двумя способами наименьшее общее кратное чисел: 35 и 10; 36 и 32; 135 и 108; 1260 и 336.

79. Любым способом найдите НОК следующих чисел: 21 и 28; 60 и 105; 4181 и 4847.

80. Найдите наименьшее общее кратное и наибольший общий делитель чисел: 6, 10 и 14. Сравните произведение трех данных чисел с произведением их наибольшего общего делителя и наименьшего общего кратного.

81. Найдите любым способом НОК чисел:

а) 120, 60 и 40; б) 54, 30 и 15;

в) 32, 36, 72 и 48; г) 70, 110, 231 и 770.

82. 1) Какой наименьшей длины должны быть доски, чтобы их можно было разрезать поперек как на куски длиной по 40 см, так и на куски длиной по 60 см, и чтобы при этом не получалось обрезков?

2) Какую наименьшую квадратную площадь можно вплотную замостить плитами, размеры которых $6\text{ дм} \times 8\text{ дм}$?

83. 1) На столе лежат книги, не более 100. Определите, сколько их, если известно, что их можно связывать в пачки по 3 книги, по 4 книги и даже по 5 книг.

2) В три школьных киоска отправили по одинаковому числу тетрадей. Для одной школы отправили тетради по 150 штук в каждой пачке, для второй — по 100 штук, а для третьей школы — по 200 штук в каждой пачке.

Сколько тетрадей отправили каждой школе, если число тетрадей наименьшее, какое может быть упаковано в целое число пачек?

84. Три теплохода заходят в порт после каждого рейса. Первый теплоход совершает рейс в 3 дня, второй — в 4 дня, а третий — в 5 дней. В понедельник они встретились в порту все вместе. Через какое наименьшее число дней встретится второй теплоход с первым; первый теплоход с третьим; второй теплоход с третьим? Через сколько дней встретятся все три теплохода и в какой это будет день недели?

85. В первом туре школьной олимпиады пятиклассникам было предложено решить дома 16 задач. За каждую верно решенную задачу ученику засчитывали 3 балла, а за неверное решение снимали 5 баллов. При подсчете оказалось, что у Миши нет ни одного балла. Сколько задач он решил верно?

86. 1) Найдите наименьшее число, которое при деле-

нии на 8 дает в остатке 7, а при делении на 9 дает в остатке 8.

2) Найдите наименьшее число, которое при делении:

на 8	дает в остатке 7,
» 7	» 6,
» 6	» 5,
» 5	» 4,
» 4	» 3,
» 3	» 2,
» 2	» 1.

§ 7. СРАВНЕНИЯ И ИХ СВОЙСТВА

I. Решение и обоснование многих задач на делимость чисел, в том числе и выводы признаков делимости, становятся яснее и проще, если пользоваться понятием сравнения и соответствующими обозначениями. Отношение сравнения было введено немецким математиком К. Гауссом, но наиболее полное и глубокое изложение теории сравнений было дано П. Л. Чебышевым в его работе «Теория сравнений».

Два числа a и b называются сравнимыми по модулю m , если при делении на m они дают один и тот же остаток.

Обозначают это так:

$$a \equiv b \pmod{m}$$

(читается: a сравнимо с b по модулю m).

Если же a и b не сравнимы по модулю m , то пишут: $a \not\equiv b \pmod{m}$.

Например: $22 \equiv 7 \pmod{5}$; $17 \equiv -4 \pmod{7}$; $10^2 \equiv 1 \pmod{11}$; $27 \not\equiv 5 \pmod{4}$.

87. Напишите несколько сравнений по модулю 6, 7, 10.

Сравнения встречаются и в повседневной жизни, например, часовая стрелка указывает время по модулю 12; минутная стрелка указывает время по модулю 60; домашний электросчетчик указывает расход электроэнергии по модулю 1000 (квт·ч).

II. Мы знаем, что два числа a и b при делении на m имеют равные остатки тогда и только тогда, если раз-

ность $a - b$ делится без остатка на m (см. № 11 и 12), следовательно:

два числа a и b сравнимы по модулю m тогда и только тогда, когда их разность $a - b$ делится на m .

Этот признак позволяет доказывать многие свойства сравнений.

88. Докажите, что a и b сравнимы по модулю m тогда и только тогда, когда $a = b + m \cdot k$, где k — целое число.

Решение. Если $a \equiv b \pmod{m}$, то $(a - b) : m$, значит, существует такое целое число k , что $a - b = k \cdot m$, откуда $a = b + km$.

Справедливо и обратное. Если $a = b + km$, то $a - b = km$, где k — целое число; значит, $(a - b) : m$, следовательно, $a \equiv b \pmod{m}$.

89. Проверьте, что: 1) Всегда $a \equiv a \pmod{m}$.

2) Если $a \equiv b \pmod{m}$, то $b \equiv a \pmod{m}$.

3) Если $a \equiv b \pmod{m}$ и $b \equiv c \pmod{m}$, то $a \equiv c \pmod{m}$.

Итак, сравнения обладают многими свойствами обычных равенств, что подчеркивается и обозначениями для сравнений. Докажем еще одно важное свойство сравнений.

Теорема. Сравнения по одному и тому же модулю можно почленно складывать, вычитать и умножать.

Доказательство. Пусть известно, что $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, тогда $a = b + k \cdot m$ и $c = d + s \cdot m$, где k и s — целые числа. Отсюда получаем:

1) $a + c = (b + d) + (k + s) \cdot m$, значит, $a + c \equiv b + d \pmod{m}$;

2) $a - c = (b - d) + (k - s) \cdot m$, значит, $a - c \equiv b - d \pmod{m}$;

3) $a \cdot c = b \cdot d + (bs + kd + ksm) \cdot m$, значит, $ac \equiv bd \pmod{m}$.

Легко видеть, что доказанная теорема справедлива для трех, четырех и более сравнений.

Следствия. 1. К обеим частям сравнения можно прибавить или вычесть одно и то же число, и обе части сравнения можно умножить на одно и то же число.

2. Члены сравнения можно переносить из одной части сравнения в другую с противоположными знаками.

3. Если $a \equiv b \pmod{m}$, то $a^k \equiv b^k \pmod{m}$, где k — любое натуральное число.

4. Пусть $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ — лю-

бой многочлен с целыми коэффициентами. Если $b \equiv c \pmod{m}$, то $P(b) \equiv P(c) \pmod{m}$, т. е. $a_n b^n + a_{n-1} b^{n-1} + \dots + a_1 b + a_0 \equiv a_n c^n + a_{n-1} c^{n-1} + \dots + a_1 c + a_0 \pmod{m}$.

III. Последнее следствие служит теоретическим основанием для вывода наиболее важных признаков делимости. Пусть некоторое число N в десятичной системе счисления изображается, считая слева направо, цифрами $a_n, a_{n-1}, \dots, a_1, a_0$, тогда можно записать:

$$N = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_1 \cdot 10 + a_0.$$

а) Так как $10 = 9 + 1$, то $10 \equiv 1 \pmod{9}$, откуда $10^k \equiv 1 \pmod{9}$. Поэтому $N \equiv a_n + a_{n-1} + \dots + a_1 + a_0 \pmod{9}$.

Следовательно, число N делится на 9 тогда и только тогда, когда на 9 делится сумма его цифр.

Аналогично получается признак делимости на 3.

б) Для любого натурального числа k очевидно, что $10^k \equiv 0$ по модулю 2, по модулю 5 и по модулю 10, значит, по каждому из них $N \equiv a_0$; получаем известные признаки делимости чисел на 2; 5 и 10.

в) Так как $10 = -1 + 11$, то $10 \equiv -1 \pmod{11}$.

По следствию 4 имеем:

$$N \equiv (-1)^n a_n + (-1)^{n-1} a_{n-1} + \dots + (-1) \cdot a_1 + a_0 \pmod{11}.$$

Следовательно, число N при делении на 11 дает тот же остаток, что и сумма его цифр, взятая с чередующимися знаками

$$M = a_0 - a_1 + a_2 - a_3 + a_4 - \dots$$

В частности, число N делится на 11 в том и только в том случае, если знакопеременная сумма его цифр делится на 11.

г) Рассмотрим остатки, получающиеся при делении на 7 последовательных степеней числа 10. Легко находим, что по модулю 7 будет $10 \equiv 3$; $10^2 \equiv 2$; $10^3 \equiv -1$; $10^4 \equiv -3$; $10^5 \equiv -2$; $10^6 \equiv 1$. Далее остатки повторяются. Следовательно, число N делится на 7 тогда и только тогда, если число $M = a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + 3a_7 + \dots$ делится на 7.

90. Определите остатки от деления на 11 следующих чисел:

$$234124; 1567394; 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19; 10! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot 9 \cdot 10.$$

91. Какие из следующих чисел делятся на 7:

234122; 1567394; 23543723?

IV. Сравнения позволяют красиво решать многие интересные задачи на делимость чисел, предлагаемые часто на олимпиадах. Рассмотрим несколько таких упражнений.

1. Найти остаток от деления числа $5^{7^{7^{\dots^7}}}$ на 6.

Решение. $5 \equiv -1 \pmod{6}$, тогда $5^k \equiv (-1)^k \pmod{6}$.

Но число $k = 7^{7^{\dots^7}}$ — нечетное, поэтому $5^k \equiv -1 \pmod{6}$.
Значит, искомый остаток равен 5.

2. Доказать, что число $22^{55} - 55^{22}$ делится на 7.

Решение. $22 \equiv 1 \pmod{7}$, значит, $22^{55} \equiv 1^{55} = 1 \pmod{7}$. $55 \equiv -1 \pmod{7}$, значит, $55^{22} \equiv (-1)^{22} = 1 \pmod{7}$. Следовательно, $22^{55} - 55^{22} \equiv 1 - 1 = 0 \pmod{7}$.

3. Доказать, что число $A = 776^{776} + 777^{777} + 778^{778}$ не делится на 3.

Решение. $776 \equiv -1 \pmod{3}$, значит, $776^{776} \equiv (-1)^{776} = 1 \pmod{3}$. $777 \equiv 0 \pmod{3}$, значит, $777^{777} \equiv 0 \pmod{3}$. $778 \equiv 1 \pmod{3}$, значит, $778^{778} \equiv 1 \pmod{3}$.

Следовательно, $A \equiv 1 + 0 + 1 \pmod{3}$, откуда следует, что при делении числа A на 3 получим остаток 2.

V. В заключение рассмотрим один из случаев, когда сравнения ведут себя иначе, чем равенства. Мы знаем, что если $ab = ac$ и $a \neq 0$, то $b = c$. Выясним, всегда ли возможно деление обеих частей сравнения на одно и то же число, т. е. всегда ли можно сравнение $ab = ac$ сокращать на множитель a .

В сравнении $35 \equiv 77 \pmod{6}$ обе части делятся на 7. Выполнив это деление, мы получим верное сравнение: $5 \equiv 11 \pmod{6}$.

В сравнении $45 \equiv 75 \pmod{6}$ обе части делятся на 15; но, выполнив это деление, мы получаем уже неверное сравнение, ибо $3 \not\equiv 5 \pmod{6}$.

Рассмотрим теперь в общем виде, когда для сравнений

имеет место правило сокращения на общий множитель, иными словами, когда из условия $ab \equiv ac$ и $a \not\equiv 0$, следует, что $b \equiv c$.

Пусть $ab \equiv ac \pmod{m}$, значит, разность $ab - ac = a(b - c)$ делится на m . Если даже $a \not\equiv m$, то нельзя утверждать, что $b - c$ делится на m . Но если числа a и m взаимно просты (см. № 153), то тогда $b - c$ обязательно должно делиться на m . Следовательно, если $ab \equiv ac \pmod{m}$ и $\text{НОД}(a, m) = 1$, то $b \equiv c \pmod{m}$.

Таким образом, обе части сравнения всегда можно разделить на одно и то же число, взаимно простое с модулем.

92. Всегда ли возможно деление обеих частей сравнения на одно и то же число в случае простого модуля?

93. Покажите, что имеет место правило сокращения на общий простой множитель, т. е. если по любому модулю m $ab \equiv ac$ и простое число a не делит m , то $b \equiv c$.

Упражнения

94. При делении на m число a дает остаток r_1 , а число b — остаток r_2 . Можно ли утверждать, что число $a \cdot b$ дает остаток $r_1 \cdot r_2$ при делении на m ? Как изменить формулировку, чтобы получилось верное утверждение?

95. Докажите следующие утверждения:

1) Если $a \equiv b \pmod{m}$, то всякий общий делитель чисел a и m будет вместе с тем и общим делителем чисел b и m , и наоборот.

2) Если $a \equiv b \pmod{m}$, то $\text{НОД}(a, m) = \text{НОД}(b, m)$.

96. Докажите, что число N делится на число m тогда и только тогда, когда сумма произведений цифр числа N на остатки, полученные от деления соответствующих степеней 10 на число m , делится на это число m .

97. Как установить, что число $100 \dots 001$, в котором число нулей четное, делится на 11?

98. Покажите, что при любом натуральном n число $5^{2n+1} \cdot 2^{n+2} + 3^{n+2} \cdot 2^{2n+1}$ делится на 19.

99. Выведите признак делимости на 13, подобный выведенному в этом параграфе признаку делимости на 7.

100. Найдите остатки от деления числа 3162819 на 11; на 7; на 13.

101. Найдите остатки от деления на 7 следующих чисел:

$$8^{61} + 6^{1050}; 13 \cdot 10^4 + 702^3 \cdot 59; 11 \cdot 18 \cdot 2322 \cdot 13 \cdot 19.$$

102. Известно, что если произведение двух чисел равно нулю, то хотя бы один из сомножителей также равен нулю. Можно ли утверждать, что если произведение двух чисел сравнимо с нулем по модулю m , то хотя бы один из сомножителей также сравним с нулем по модулю m ?

103. Докажите, что если произведение двух чисел сравнимо с нулем по простому модулю p , то хотя бы один из сомножителей также сравним с нулем по модулю p .

§ 8. ВЫЧЕТЫ. ТЕОРЕМА ФЕРМА

I. Возьмем натуральное число $m = 6$ и будем (мысленно!) делить на 6 все целые числа. Группируя числа по остаткам, получим шесть различных классов чисел, объединенных нами в столбцы:

— 12,	— 11,	— 10,	— 9,	— 8,	— 7,
— 6,	— 5,	— 4,	— 3,	— 2,	— 1,
0,	1,	2,	3,	4,	5,
6,	7,	8,	9,	10,	11,
12,	13,	14,	15,	16,	17,

В каждом столбце любые два числа сравнимы между собой по модулю 6, но никакие два числа из разных столбцов не сравнимы по модулю 6.

Рассмотрим теперь произвольное натуральное число m . Любые два числа b и c , сравнимые по модулю m с одним и тем же числом a , сравнимы между собой, поэтому можно все числа, сравнимые с данным числом a по модулю m , объединять в один класс сравнимых между собой чисел. В результате все целые числа разбиваются на классы по модулю m , причем числа одного и того же класса сравнимы между собой по модулю m , но никакие два числа разных классов не сравнимы по модулю m .

Число таких классов по модулю m равно m , ибо числа одного класса при делении на m дают один и тот же остаток, а остатками могут быть лишь следующие m чисел: $0, 1, 2, \dots, m - 1$.

Выберем произвольным образом по одному числу (представителю) в каждом из классов. Получим группу из t чисел, никакие два из которых не сравнимы между собой по модулю t , но любое целое число сравнимо по модулю t с одним из чисел этой группы. Такую группу чисел называют *полной системой вычетов по модулю t* .

Например, по модулю 6 полными системами вычетов являются группы чисел: (0, 1, 2, 3, 4, 5); (—6, 7, 2, —9, 10, 17) и другие. Очевидно, что полных систем вычетов по любому модулю существует бесконечное множество.

104. Напишите по две полные системы вычетов по модулям 3, 7 и 10.

II. Так как во многих вопросах теории делимости числа одного и того же класса могут заменять друг друга, то можно избирать всякий раз наиболее целесообразную полную систему вычетов. Иногда выгодно большие числа заменять меньшими неотрицательными числами или вычетами брать отрицательные числа.

Например, требуется установить делимость числа $N = 166^3 \cdot 320^2 + 10^4 \cdot 2^{20} + 89$ на 13. Нет необходимости выполнять указанные действия и получившийся результат делить на 13. Можно выполнять действия не над самими числами, а над их вычетами по модулю 13.

166 можно заменить вычетами 10 или —3; 320 — вычетами 8 или —5; $2^4 = 16$ заменяем вычетом 3 и т. д. Число N при делении на 13 даст тот же остаток, что и число

$$N_1 = (-3)^3 \cdot (-5)^2 + (-3)^4 \cdot 3^5 - 2.$$

Если заметить, что $3^3 = 27$ можно заменить вычетом 1, а $5^2 = 25$ — вычетом —1, то легко найти остаток от деления числа N на 13: $-1 \cdot (-1) + 1 - 2 = 0$.

Возможны и иные приложения такой арифметики вычетов. Надо, например, доказать, что число $n^5 - n$ при любом целом n делится на 5. Возьмем полную систему вычетов по модулю 5 в виде (—2, —1, 0, 1, 2). Легко проверить, что при любом значении n из этих пяти вычетов $n^5 - n$ равно числу, делящемуся на 5. Следовательно, $n^5 - n$ делится на 5 при любом целом n .

105. Докажите, что $n^7 - n$ при любом целом n делится на 7.

III. Выясним теперь, когда значения произведения

$a \cdot x$ образуют полную систему вычетов по модулю m , если x пробегает полную систему вычетов по модулю m .

Пусть $m = 6$ и $a = 5$. Будем придавать x значения 0, 1, 2, 3, 4, 5. Тогда получим, что по модулю 6: $5 \cdot 0 \equiv 0$; $5 \cdot 1 \equiv 5$; $5 \cdot 2 \equiv 4$; $5 \cdot 3 \equiv 3$; $5 \cdot 4 \equiv 2$; $5 \cdot 5 \equiv 1$. Следовательно, значения произведения $5 \cdot x$ также образуют полную систему вычетов по модулю 6.

Возьмем $a = 4$ при том же значении $m = 6$. Очевидно, что $4 \cdot 0 \equiv 0$; $4 \cdot 1 \equiv 4$; $4 \cdot 2 \equiv 2$; $4 \cdot 3 \equiv 0$; $4 \cdot 4 \equiv 4$ и $4 \cdot 5 \equiv 2$ по модулю 6. В этом случае мы уже не получим полной системы вычетов по модулю 6.

106. Проверьте для модуля $m = 4$, в каком случае значения произведения ax образуют полную систему вычетов, если x пробегает полную систему вычетов по модулю 4, беря $a = 3$ и $a = 6$.

Теорема. Если числа a и m взаимно просты и в выражении ax число x пробегает полную систему вычетов по модулю m , то и полученные значения этого выражения образуют полную систему вычетов по модулю m .

Доказательство. Так как x принимает m значений, то и для ax получим ровно m значений. Чтобы утверждать, что они образуют полную систему вычетов, надо показать, что никакие два из них не сравнимы по модулю m . Предположим, что для некоторых двух чисел x_1 и x_2 , принадлежащих разным классам по модулю m , $ax_1 \equiv ax_2 \pmod{m}$. Но a взаимно просто с m , поэтому обе части сравнения можно разделить на a , тогда должно быть $x_1 \equiv x_2 \pmod{m}$, чего быть не может. Таким образом, теорема доказана.

IV. При решении упражнений на делимость чисел, содержащих большие показатели степеней, удобно применять так называемую «малую теорему Ферма».

Если p — простое число, не делящее целого числа a , то $a^{p-1} \equiv 1 \pmod{p}$.

Доказательство. Рассмотрим числа, кратные a :

$$n_1 = a; n_2 = 2a; n_3 = 3a; \dots; n_{p-1} = (p-1)a.$$

Никакие два из них не сравнимы между собой по модулю p , ибо в противном случае их разность $n_k - n_s = ka - sa = a(k-s)$ делилась бы на p , чего быть не может. Действительно, p — число простое и по условию a не делится на p ; с другой стороны, и $k-s$ не может делиться на p , ибо

$1 \leq s < k \leq p-1$, значит, $0 < k-s < p$. Значит, и произведение $a(k-s)$ не делится на p .

Аналогично устанавливается, что ни одно из выписанных чисел n не делится на p .

Следовательно, числа n_1, n_2, \dots, n_{p-1} образуют полную систему вычетов по модулю p , отсутствует лишь нуль. Поэтому они сравнимы с числами $1, 2, \dots, p-1$, взятыми, быть может, в некоторой их перестановке. Тогда $n_1 \cdot n_2 \cdot \dots \cdot n_{p-1} = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) a^{p-1} \equiv 1 \cdot 2 \times 3 \cdot \dots \cdot (p-1) \pmod{p}$.

Но число $k = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1)$ не делится на простое число p , поэтому обе части сравнения можно сократить на число k , получим:

$$a^{p-1} \equiv 1 \pmod{p}.$$

107. Проверьте, что $10^6 \equiv 1 \pmod{7}$;

$$5^{10} \equiv 1 \pmod{11}; 4^{22} \equiv 1 \pmod{23}.$$

Решение. Рассмотрим вычисления при $a=4$ для модуля $p=23$. По модулю 23 имеем: $4^2 \equiv -7$; $4^3 = 4^2 \times 4 \equiv -28 \equiv -5$; $4^4 = 4^3 \cdot 4 \equiv -20 \equiv 3$; $4^8 = 4^4 \cdot 4^4 \equiv 9$; $4^{11} = 4^8 \cdot 4^3 \equiv -45 \equiv 1$; $4^{22} = (4^{11})^2 \equiv 1$.

Из приведенного решения видно, что иногда не только $(p-1)$ -я степень, но и более низкая степень a оказывается сравнимой с единицей. Но можно доказать, что наименьшая степень k такая, что $a^k \equiv 1 \pmod{p}$ обязательно является делителем числа $p-1$ (см. № 172).

Следствие. Если p — простое число, то для любого целого числа a имеем $a^p \equiv a \pmod{p}$, иными словами, разность $a^p - a$ делится на p .

Действительно, если a делится на p , то утверждение очевидно. Если же a не делится на p , то по теореме Ферма $a^{p-1} \equiv 1 \pmod{p}$. Умножив почленно на a , получим требуемое сравнение.

Применим теорему Ферма к решению задачи: «Найти остаток от деления на 5 числа 1967^{1971} ».

Очевидно, что $1967 \equiv 2 \pmod{5}$, значит, $1967^{1971} \equiv 2^{1971} \pmod{5}$. Но $2^4 \equiv 1 \pmod{5}$, поэтому найдем остаток от деления 1971 на 4, получим $2^{1971} = 2^{4 \cdot 492 + 3} = (2^4)^{492} \times 2^3 \equiv 1 \cdot 2^3 \pmod{5}$. Так как $2^3 \equiv 3 \pmod{5}$, то искомый остаток равен 3.

Рассмотрим решение еще одной задачи: «Может ли быть точным квадратом число, сумма цифр которого 1970?»

Пусть существует такое число n , что сумма цифр у n^2 равна 1970. Так как $1970 \equiv 2 \pmod{3}$, то и $n^2 \equiv 2 \pmod{3}$. Очевидно, что n не $\div 3$, но тогда по теореме Ферма должно быть $n^2 \equiv 1 \pmod{3}$. Одновременно не могут иметь места сравнения $n^2 \equiv 2$ и $n^2 \equiv 1$. Следовательно, число, сумма цифр которого 1970, не может быть точным квадратом.

Примечание. Имеет место более общая теорема Эйлера: *если a взаимно просто с m , то $a^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ равно числу натуральных чисел, не больших m и взаимно простых с m (см. № 174).*

Упражнения

108. Напишите полные системы вычетов по модулю 6, состоящие:

- а) из наименьших положительных чисел;
- б) из наименьших неотрицательных чисел;
- в) из наименьших по абсолютной величине чисел.

109. В арифметике вычетов по некоторому модулю числа $3 \cdot 5$; $4 \cdot 4$ и $6 \cdot 4$ заменили соответственно вычетами 1, 2 и 3. Найдите неизвестный модуль.

110. Если числа a и m взаимно просты и в выражении $ax + b$ число x пробегает полную систему вычетов по модулю m , то и получаемые значения этого выражения образуют полную систему вычетов по модулю m . Докажите.

111. Проверьте, что $2^8 \equiv 1 \pmod{17}$;

$3^8 \equiv -1 \pmod{17}$; $3^{14} \equiv -1 \pmod{29}$; $5^{14} \equiv 1 \pmod{29}$.

112. Проверьте теорему Ферма, взяв $p = 5, 7, 11$ и придавая a различные значения.

113. Найдите остаток от деления числа $1971^{1971} - 1967^{1967}$ на 7.

§ 9. УРАВНЕНИЯ В ЦЕЛЫХ ЧИСЛАХ

I. Нередко при решении задач составлением уравнений требуется не вообще решить уравнение, а найти целочисленные значения неизвестных, причем коэффициенты в таких уравнениях также целые числа. Решение

уравнений в целых числах, наряду с делимостью чисел, является одним из наиболее интересных вопросов теории чисел.

Решением таких уравнений занимались видные математики древности, такие, как греческий математик Пифагор (VI век до н. э.), александрийский математик Диофант (II—III век н. э.), по имени которого уравнения в целых числах называются диофантовыми уравнениями. Этой труднейшей проблемой теории чисел занимались и такие крупные математики, как П. Ферма, Л. Эйлер и другие. Но и на сегодняшний день нет общих методов решения таких уравнений.

Решение диофантовых уравнений первой степени с двумя неизвестными вида $ax + by = c$ теснейшим образом связано с решением сравнений с неизвестным. Действительно, это уравнение можно записать в виде двух сравнений: $ax \equiv c \pmod{b}$ или $by \equiv c \pmod{a}$. Наоборот, сравнение $ax \equiv c \pmod{b}$ приводит к уравнению в целых числах $ax - c = by$.

II. Рассмотрим подробно решение сравнений вида $ax \equiv c \pmod{b}$, содержащих неизвестное в первой степени. Очевидно, что если число x_0 удовлетворяет данному сравнению, то и любое число x , сравнимое с x_0 по модулю b , также будет ему удовлетворять. Поэтому обычно решением (или корнем) сравнения называют не отдельное число, а целый класс (по модулю b) чисел, удовлетворяющих данному сравнению.

Если число a взаимно просто с модулем b и если x пробегает полную систему вычетов по этому модулю, то по доказанной ранее теореме соответствующие значения ax будут тоже образовывать полную систему вычетов по модулю b . Поэтому одно из них и только одно будет сравнимо с c . Следовательно, мы получим и притом только один класс решений данного сравнения.

Решениями сравнения $ax \equiv c \pmod{b}$ являются такие целые числа x , что $c - ax$ делится на b , значит $c - ax = by$ или $ax + by = c$, где y — целое число. Полученный нами результат о решении сравнений можно применить к уравнениям в целых числах.

Если числа a и b взаимно просты, то уравнение $ax + by = c$ всегда может быть решено в целых числах. Если (x_0, y_0) есть одно из его решений, то все решения могут быть записаны так:

$$x = x_0 + bk; y = y_0 - ak,$$

где k — любое целое число.

114. Решить в целых числах уравнение:

$$5x - 8y = 13.$$

Решение. Заменим это уравнение сравнением $-8y \equiv 13 \pmod{5}$ или $2y \equiv 3 \pmod{5}$. Очевидно, что $y_0 = 4$ удовлетворяет этому сравнению, после чего легко найти $x_0 = 9$, а все решения даются формулами: $x = 9 - 8k$; $y = 4 - 5k$, где k — любое целое число.

115. Решите следующие диофантовы уравнения:

а) $3x + 4y = 5$; б) $7x + 8y = 3$.

Рассмотрим случай, когда a и b имеют наибольший общий делитель $d > 1$. Пусть $a = d \cdot a_1$; $b = d \cdot b_1$, причем $\text{НОД}(a_1, b_1) = 1$.

Если c не делится на d , то уравнение $ax + by = c$ не может иметь решений, ибо допустив, что при некоторых целых x_0 и y_0 будет $ax_0 + by_0 = c$, то тогда слагаемые ax_0 и by_0 делились бы на d , а их сумма, число c , не делится на d .

Если же c делится на d , то $c = dc_1$, и уравнение $ax + by = c$ можно заменить ему равносильным уравнением $a_1x + b_1y = c_1$, у которого коэффициенты при неизвестных уже взаимно просты, а такие уравнения мы умеем решать. Следует учесть, что в этом случае все решения даются формулами:

$$x = x_0 + k \cdot b_1; y = y_0 - k \cdot a_1.$$

116. Решите следующие уравнения в целых числах
а) $3x + 6y = 22$; б) $14x + 22y = 26$.

III. Иногда по условию задачи требуется найти не любые целые числа, а такие, которые удовлетворяют некоторым дополнительным условиям. Например, требуется найти все целые положительные значения x и y , удовлетворяющие уравнению: $3x + 5y = 19$.

Решая это уравнение, мы найдем, что $x = 3 + 5k$, $y = 2 - 3k$. Но k не может быть любым целым числом, ибо надо, чтобы $x > 0$ и $y > 0$, т. е. $3 + 5k > 0$ и $2 - 3k > 0$, откуда находим, что $k > -\frac{3}{5}$ и $k < \frac{2}{3}$.

Значит, k может принимать только одно целое значение: $k = 0$, а тогда $x = 3$; $y = 2$. Никаких других целых положительных решений уравнение не имеет.

117. Найдите все целые положительные значения x и y , удовлетворяющие следующим уравнениям: а) $3x + 2y = 5$; б) $5x + 7y = 112$.

118. Трехзначное число оканчивается цифрой 7. Если переставить эту цифру на первое место, то получится число, в два раза и еще на 21 единицу большее первоначального. Определите это число.

119. Найдите двузначное число, которое в 8 раз больше суммы своих цифр.

IV. Решение некоторых задач сводится к решению в целых числах систем двух уравнений с тремя неизвестными. Такие системы обычно решаются методом последовательного исключения неизвестных: исключая одно из неизвестных, получим одно уравнение с двумя неизвестными. Рассмотрим, в качестве примера, такую задачу:

«Можно ли на 100 копеек купить 100 предметов: карандашей (цветных и простых) и перьев, если известно, что цветной карандаш стоит 5 коп., простой — 3 коп., а перьев продают 3 штуки на одну копейку?»

Решение. Обозначив число цветных карандашей через x , простых карандашей — через y и перьев — через z , легко составить два уравнения: $x + y + z = 100$ и $5x + 3y + \frac{z}{3} = 100$.

Следовательно, получили систему двух уравнений с тремя неизвестными:

$$\begin{cases} x + y + z = 100; \\ 15x + 9y + z = 300, \end{cases}$$

где x , y и z — целые неотрицательные числа, не большие 100.

Исключив z , получим одно уравнение с двумя неизвестными:

$$14x + 8y = 200 \text{ или } 7x + 4y = 100,$$

$$y = \frac{100 - 7x}{4} = 25 - x - \frac{3x}{4}.$$

Очевидно, что x должно быть кратно 4, причем $7x = 100 - 4y$, поэтому $7x < 100$, то есть $x \leq 14$.

Вычислив значения y и z при $x = 0; 4; 8; 12$, получим четыре различных ответа: $(0; 25; 75)$, $(4; 18; 78)$, $(8; 11; 81)$ и $(12; 4; 84)$.

Если считать, что первый ответ не подходит по смыслу задачи, то требуемая покупка может быть произведена только тремя способами.

Упражнения

120. Решите следующие сравнения:

а) $5x \equiv 4 \pmod{7}$; б) $6x \equiv 5 \pmod{15}$; в) $6x \equiv 3 \pmod{15}$.

121. Решите следующие уравнения в целых числах:

а) $3x - 4y = 29$; б) $91x - 65y = 42$.

122. Если между цифрами двузначного числа вписать нуль, то полученное трехзначное число будет в 7 раз больше первоначального. Найдите это число.

123. Если к двузначному числу приписать слева и справа по единице, то полученное четырехзначное число будет больше первоначального в 21 раз. Найдите это число.

124. Библиотека на 20 рублей купила 20 книг трех видов: по 3 рубля, по 2 рубля и 50 копеек за книгу. Сколько книг каждого вида купила библиотека?

125. Докажите, что сравнение $ax \equiv b \pmod{p}$, где p — число простое и $a \not\equiv 0 \pmod{p}$, всегда имеет в точности одно решение. Убедитесь, что $x \equiv ba^{p-2} \pmod{p}$ является решением.

§ 10. ЗАДАЧИ ПОВЫШЕННОЙ ТРУДНОСТИ

126. Докажите, что если $a : b$ и $b : a$, то $a = \pm b$.

127. Докажите, что: 1) Сумма пяти последовательных целых чисел делится на 5. 2) Произведение пяти последовательных целых чисел делится на 5.

128. Докажите, что $a^5 - a$ делится на 5 при любом целом a .

129. 1) Может ли сумма нечетных чисел быть числом четным? 2) Каким числом, четным или нечетным, будет сумма нечетного числа слагаемых, каждое из которых есть число нечетное?

130. Члены футбольной команды пионерского лагеря перед отъездом домой решили обменяться друг с другом фотографиями. Каким числом, четным или нечетным, будет общее число фотографий, которыми обменялись ребята?

Сколько было таких фотографий, если в обмене участвовало 11 человек?

131. 1) 31 августа на школьном дворе встретилось 7 пятиклассников. Некоторые из них обменялись рукопожатиями. Докажите, что хотя бы один из них пожал руку четному числу друзей.

Примечание. Нуль — число четное, поэтому ученик, ни с кем не поздоровавшийся за руку, сделал четное число рукопожатий.

2) В розыгрыше приза «Кожаный мяч» участвовало большое число футбольных детских команд в каждой возрастной группе. Некоторые из них провели четное число матчей, другие — нечетное число матчей. Каким числом, четным или нечетным, будет число команд, которые провели нечетное число матчей?

132. В одной рукописи приведено описание города, расположенного на 8 островах. Острова между собой и с материком были соединены мостами. На материк выходило 5 мостов; на 4 островах берут начало по 4 моста; на 3 островах берут начало по 3 моста и на один остров можно пройти только по одному мосту.

Почему такого расположения мостов быть не может?

133. Если сумма двух чисел оканчивается нулем, то разность квадратов этих чисел делится на 10. Докажите.

134. Можно ли число 1970 представить в виде разности квадратов двух целых чисел?

135. Число, записанное в десятичной системе, оканчивается нулем. Будет ли это число оканчиваться нулем: 1) В пятеричной системе? 2) В троичной системе? 3) Будет ли оно кратно 5, если его записать в восьмеричной системе?

136. Вместо точек поставьте такие цифры, чтобы каждое из чисел: $1011\cdot_2$; $12\cdot_3$; $34\cdot_{21_5}$; $345\cdot_6$ делилось на 2.

137. Какие цифры можно поставить вместо точек, чтобы каждое из чисел: $1\cdot_3$ и $5\cdot_{26_7}$ было четным?

138. Вместо точек поставьте такие цифры, чтобы каждое из чисел: $201\cdot_3$; $120\cdot_0_3$; $4\cdot_{34_7}$; $336\cdot_9$ делилось на 3.

139. Вместо точек поставьте такие цифры, чтобы каждое из чисел: $32\cdot_5$; $2\cdot_{40_5}$; $1\cdot_{5_6}$; $3\cdot_{34_6}$ делилось на 5.

140. Вместо точек поставьте такие цифры, чтобы каждое из чисел: $642\cdot_3$; $2313\cdot_4$ делилось и на 2 и на 3.

141. 1) Можно ли из одних «двоек» составить число $(2; 22; 222; 2222; \dots)$, которое делится на 9? на 5?

2) Можно ли в семеричной системе из одних «пятерок» составить число $(5; 55; 555; \dots)$, делящееся на 3?

142. Выведите признаки делимости чисел на 4; 25; 50, считая основанием системы счисления $d = 100$.

143. Выведите общий признак делимости на 7, 11 и 13, считая основанием системы счисления $d = 1000$.

144. A — 1970-значное число, делящееся на 9; B — сумма цифр числа A ; B — сумма цифр числа B .

Найдите сумму цифр числа B .

145. Докажите, что нет таких чисел, которые от перестановки начальной цифры в конец числа увеличивались бы ровно в 5 раз.

146. Найдите такое целое число, которое в 7 раз больше цифры единиц этого числа.

147. Докажите, что число вида $n^4 + 4$ есть составное при любом целом n , большем единицы.

148. Существуют сколь угодно длинные участки натурального ряда, вовсе не содержащие простых чисел и, следовательно, сплошь состоящие из чисел составных. Докажите.

149. Докажите, что два соседних целых числа n и $n + 1$ всегда являются взаимно простыми.

150. Докажите, что если $a - b = 2$ и числа a и b не являются взаимно простыми, то $\text{НОД}(a, b) = 2$.

151. Докажите, что каковы бы ни были натуральные числа a и b , всегда можно подобрать два таких целых числа x и y , что $ax + by = \text{НОД}(a, b)$.

152. Для того чтобы числа a и b были взаимно простыми, необходимо и достаточно, чтобы существовали два таких целых числа x и y , что $ax + by = 1$. Докажите.

153. Если числа a и p взаимно простые и произведение $a \cdot b$ делится на p , то b делится на p . Докажите.

154. Верно ли утверждение, что если произведение $a \cdot b$ делится на p , то один из сомножителей делится на p ? Приведите примеры, подтверждающие это.

155. Докажите следующие утверждения:

1) Если p простое число, то любое натуральное число a либо делится на p , либо взаимно просто с ним.

2) Если произведение $a \cdot b$ делится на простое число p , то по крайней мере один из сомножителей делится на p .

3) Если произведение нескольких чисел делится на простое число p , то по крайней мере один из сомножителей делится на p .

156. Докажите единственность разложения любого натурального числа на простые множители, то есть что всякое составное число может быть представлено как произведение простых множителей единственным образом, если не учитывать порядка множителей.

157. Применяя задачу № 153, установите, что если число a делится порознь на два числа p и q , которые взаимно просты, то a делится на их произведение pq .

158. Сформулируйте признаки делимости чисел на 6, 12 и 15.

159. Докажите следующие утверждения:

1) Произведение трех последовательных целых чисел делится на 6.

2) Произведение четырех последовательных целых чисел делится на 24.

3) Произведение пяти последовательных целых чисел делится на 120.

160. Установите, что если a целое число, то

1) $a^3 - a$ делится на 6.

2) $a^5 - a$ делится на 30.

3) $a(a^2 + 5)$ делится на 6.

4) $a^5 - 5a^3 + 4a$ делится на 120.

5) $\frac{a}{3} + \frac{a^2}{2} + \frac{a^3}{6}$ есть целое число.

6) $\frac{a^4}{24} + \frac{a^3}{4} + \frac{11a^2}{24} + \frac{a}{4}$ есть целое число.

161. Докажите, что всякое общее кратное чисел a и b делится на $m = \text{НОК}(a, b)$.

162. Докажите, что всякий делитель d числа $N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n}$ имеет вид $d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_n^{\beta_n}$, где $0 \leq \beta_1 \leq \alpha_1$; $0 \leq \beta_2 \leq \alpha_2$; ...; $0 \leq \beta_n \leq \alpha_n$.

163. Найдите число всех различных делителей числа

$$N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n}.$$

164. Дайте строгое обоснование известных вам способов отыскания НОД(a, b) и НОК(a, b) разложением a и b на простые множители.

165. При делении числа на 2 в остатке получается 1, а при делении на 3 — остаток 2. Какой будет остаток, если это число разделить на 6?

166. 1) Найдите наименьшее число, которое при делении на 3 дает в остатке 2, при делении на 5 дает в остатке 3 и при делении на 7 — снова 2.

2) Найдите наименьшее число, которое кратно 7, но при делении на 3, на 4 и на 5 дает в остатке 1.

167. 1) Вместо точек поставьте такие цифры, чтобы числа 8. и 1. 4 делились и на 3 и на 4.

2) Вместо точек поставьте такие цифры, чтобы каждое из чисел: 2. . и 86. . делилось одновременно и на 5, и на 9.

168. 1) Из цифр 0, 2, 3 и 4 составьте четырехзначные числа, которые делились бы на 4, на 5 и на 9 (одновременно).

2) Из цифр 5, 8, 4 и 1 составьте несколько четырехзначных чисел, которые делились бы на 4, на 5 и на 9.

169. Сколько натуральных чисел, не больших 500 и не делящихся ни на 2, ни на 3?

170. Найдите остаток от деления числа $57^{7^{7^{\cdot^{\cdot^{\cdot^7}}}}}$ на 7.

171. Делятся ли числа $222^{555} + 555^{222}$ и $2222^{5555} + 5555^{2222}$ на 7?

172. Докажите, что наименьшее натуральное число k , для которого $a^k \equiv 1 \pmod{p}$ (где p — простое число, не делящее a), должно быть делителем $p-1$.

173. Мы знаем, что если одно из чисел данного класса вычетов по модулю m взаимно просто с m , то и все числа этого класса взаимно просты с m (см. № 95). Поэтому можно говорить о классах, взаимно простых с модулем. Группа чисел, содержащая по одному представителю от каждого класса, взаимно простого с модулем, называется приведенной системой вычетов по данному модулю.

Докажите, что если числа a и m взаимно просты и если в выражении ax число x пробегает какую-либо приведенную систему вычетов по модулю m , то и получаемые значения выражения ax образуют приведенную систему вычетов по модулю m .

174. Докажите теорему Эйлера: если числа a и b взаимно просты, то $a^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ равно числу натуральных чисел, не больших m и взаимно простых с m .

175. Найдите остаток от деления числа 127^{107} на 15.

176. Решить диофантовы уравнения:

а) $11x + 12y = 58$; б) $153x - 34y = 51$.

177. Найдите трехзначное число, которое в 11 раз больше суммы своих цифр.

178. Даны три разные цифры. Сумма всех трехзначных чисел, какие только можно составить, комбинируя эти три цифры, равна 2886. Если расположить данные цифры по убыванию их значений и из полученного числа вычесть число, составленное из этих же цифр, но взятых в обратном порядке, то разность составит 495. Найдите эти три цифры, если известно, что среди них нет нуля.

179. В учреждении стоят 14 канцелярских столов с одним, двумя, тремя и четырьмя ящиками. Всего в столах 33 ящика. Сколько столов с одним ящиком, если известно, что их столько, сколько с двумя и тремя ящиками вместе?

180. Люда с мамой делали покупки. У них было немного менее 150 рублей, причем только пятерками и рублями. По возвращении домой у них осталось ровно треть первоначальной суммы, при этом пятерок стало столько, сколько раньше было рублей, а рублей столько, сколько раньше было пятерок. Сколько денег они истратили на покупку?

181. В шахматном турнире участвовало два ученика седьмого класса и несколько восьмиклассников. Два семиклассника набрали вместе 8 очков, а каждый восьмиклассник набрал одно и то же число очков. Сколько восьмиклассников участвовало в турнире?

Ответы и решения

1. б) 6 и 1; 9 и 4; -18 и 3; -10 и 9.

4. $|a|$.

5. Наибольший положительный делитель числа a есть $|a|$, значит, если $a : b$, где $b > 0$, то $b \leq |a|$. Но различных натуральных чисел, не больших $|a|$, только лишь $|a|$.

11. Пусть $a = bq_1 + r_1$ и $c = bq_2 + r_2$, причем $r_1 = r_2$. Тогда $a - c = (bq_1 + r_1) - (bq_2 + r_2) = b(q_1 - q_2)$.

12. Известно, что $a - c = bq$. Пусть $c = bq_1 + r$, где $0 \leq r < b$, тогда $a = c + bq = bq_1 + r + bq = b(q_1 + q) + r$, где $0 \leq r < b$, значит, r есть остаток от деления a на b .

15. 4) Двухзначное число, у которого цифра десятков a и цифра единиц b , содержит $10a + b$ единиц. Число, записанное теми же цифрами, но в обратном порядке, есть $10b + a$. Их сумма $(10a + b) + (10b + a) = 11a + 11b = 11(a + b)$.

16. Если $N_1 = 100a + 10b + c$, то обращенное число $N_2 = 100c + 10b + a$. Значит, $N_1 - N_2 = (100a + 10b + c) - (100c + 10b + a) = 99a - 99c = 99(a - c)$.

18. 1) Рассматриваем два случая: $n = 2k$ — число четное и $n = 2k + 1$ — число нечетное.

2) Рассматриваем три возможных случая: число n делится на 3, значит, $n = 3k$; число n при делении на 3 дает остаток 1, значит, $n = 3k + 1$; число n при делении на 3 дает остаток 2, значит, $n = 3k + 2$.

20. 2) Возьмем два последовательных нечетных числа: $n_1 = 2k - 1$ и $n_2 = 2k + 1$, тогда $n_1^2 - n_2^2 = (2k - 1)^2 - (2k + 1)^2 = 4k(-2) = 8(-k)$.

21. 5643; 14 014; 5 069 812; 4 192 716.

22. 2348; 483 568.

25. 1) 0 или 5; любую цифру; такую цифру найти нельзя.

2) 1; 2; 7.

3) 0, 3, 6 или 9; 2, 5 или 8; 2, 5 или 8.

26. 1) 401, остальные делятся на 5.

2) 366, остальные делятся на 9.

3) 342, остальные делятся на 4.

27. Всякий раз число кусков увеличивалось на 5, поэтому общее число кусков должно делиться на 5.

28. Те и только те числа, которые оканчиваются цифрой 0.

29. Те и только те числа, которые оканчиваются четной цифрой.

30. 1) Те и только те числа, которые оканчиваются нулем или цифрой 4.

2) Те и только те числа, которые оканчиваются нулем или цифрой 3.

31. Те и только те числа, у которых сумма цифр делится на данное число.

32. Те и только те числа, у которых сумма цифр делится на данное число.

33. 1010_2 ; 1001_3 ; 213_5 ; 1100_7 ; 5604_8 .

34. 220_3 ; 312_4 ; 231_7 ; 483_9 .

35. 320_5 ; 523_6 .

36. 2010_7 ; 4640_7 ; 25_8 ; 4730_8 .

38. Пусть наименьший отличный от единицы положительный делитель составного числа N есть p , значит, $N = p \cdot q$, где $q \geq p$. Тогда $p^2 = p \cdot p \leq p \cdot q = N$, то есть $p^2 \leq N$.

39. Если бы число N было составным, то оно имело бы наименьший простой делитель, квадрат которого не больше N .

40. Достаточно проверить для 2, 3, 5 и 7, ибо $11^2 > 100$.

41. По теореме Чебышева, для каждого натурального числа n существует простое число, большее его. Но так как n может быть сколь угодно большим числом, следовательно, наибольшего простого числа быть не может.

47. 1) Да, например: $3 + 2$; $11 + 2$ и другие числа-близнецы.

2) Нет, ибо сумма таких простых чисел (нечетных!) есть всегда число четное.

49. Простое число p может делиться только на 1 и на p . Но q — число простое, оно не равно 1, значит, $q = p$.

50. $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30\,031 = 59 \cdot 509$; остальные все числа простые.

51. Разложим сначала на простые множители все составные множители, а затем соберем все простые множители, складывая соответствующие показатели степеней. Получим

$$10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7.$$

52. В десятой степени.
53. В четвертой степени.
54. Четырьмя нулями.
55. 24 нулями.
56. 1) 8; 2) 16; 3) 16.
57. 1) 1, 2, 3, 5, 6, 9, 10, 15, 18, 30, 45, 90.
2) 1, 2, 5, 7, 4, 10, 14, 35, 20, 28, 70, 140.
58. 1) 1, 2, 5, 10.
2) По 1, по 2, по 5 или по 10 учащихся в один ряд.
59. 10.
60. 1) 6; 2) 60.
61. 6; 9; 8; 16.
62. 35.
63. 12; 6; 4; 3; 2; 1.
64. 1) 1; 2; 3; 5; 6; 10; 15; 30.
2) 1; 3; 9; 27; 81.
65. а) 1; 2; 4; 8. б) 1; 2; 3; 4; 6; 9; 12; 18; 36. в) 1; 2; 3; 4; 5; 6; 8; 10; 12; 15; 20; 24; 25; 30; 40; 50; 60; 75; 100; 120; 150; 200; 300; 600.
66. а) $4 \times 3 = 12$ делителей; б) $4 \times 5 = 20$ делителей;
в) $(k+1) \cdot (n+1)$ делителей.
67. 12; 60; 17.
71. 1) 15; 14; 13; 1; 23; 1.
2) 6; 1; 7; 105.
72. 7; 16; 128.
73. 1) 8 км/ч; 2) 23 часа.
74. 9, 12 и 10 вагонов.

75. По доказанному первому утверждению $\frac{ab}{D} = M$ есть общее кратное чисел a и b . По второму утверждению $\frac{ab}{m} = d$ есть общий делитель чисел a и b . Следовательно, $ab = MD$ и $ab = md$, откуда $MD = md$.

$D = \text{НОД}(a, b)$, значит, $D \geq d$, но тогда $M \leq m$, что возможно лишь в том случае, когда $M = m$, ибо m — наименьшее общее кратное.

78. 70; 288; 540; 5040.
79. 84; 420; 547 711.
81. 120; 270; 288; 2310.
82. 1) 120 см; 2) $24 \text{ дм} \times 24 \text{ дм}$.
83. 1) 60 книг; 2) 600 тетрадей.
84. Все три встретятся через 60 дней, в пятницу.
85. 10 задач.

86. 1) НОК (8,9) — 1 = 72 — 1 = 71.

2) НОК (8, 7, 6, 5, 4, 3, 2) — 1 = 839.

90. 0; 4; 0; 10.

91. 234 122 и 23 543 723.

92. Всегда, кроме деления на число, сравнимое с нулем по данному модулю.

93. Так как a — число простое, то a и m взаимно просты.

94. Может оказаться, что $r_1 \cdot r_2 \geq m$, поэтому можно лишь утверждать, что остаток произведения сравним с произведением остатков по модулю m .

95. Достаточно сравнение $a \equiv b \pmod{m}$ заменить эквивалентным ему утверждением, что $a = b + km$.

97. Применить признак делимости на 11.

98. $5^{2n+1} \cdot 2^{n+2} + 3^{n+2} \cdot 2^{2n+1} = (5^2)^n \cdot 5 \cdot 2^n \cdot 2^2 + 3^n \cdot 3^2 \times$
 $\times (2^2)^n \cdot 2 = 20 \cdot 25^n \cdot 2^n + 18 \cdot 3^n \cdot 4^n = 20 \cdot 50^n + 18 \cdot 12^n$. Но по модулю 19 имеем: $20 \equiv 1$; $18 \equiv -1$ и $50 \equiv 12$, поэтому $20 \cdot 50^n + 18 \cdot 12^n \equiv 1 \cdot 12^n - 1 \cdot 12^n = 0 \pmod{19}$.

100. Остатки соответственно равны: 0; 2; 10.

101. По модулю 7 можно записать:

$$8^{61} + 6^{1050} \equiv 1^{61} + (-1)^{1050} = 2.$$

$$13 \cdot 10^4 + 702^3 \cdot 59 \equiv -1 \cdot 3^4 + 2^3 \cdot 3 = -81 + 24 =$$
$$= -57 \equiv 6.$$

$$11 \cdot 18 \cdot 2322 \cdot 13 \cdot 19 \equiv 4 \cdot 4 \cdot 5 \cdot (-1) \cdot 5 = -20^2 \equiv -$$
$$-(-1)^2 = -1 \equiv 6.$$

102. Нельзя. Например: $3 \cdot 4 \equiv 0 \pmod{6}$, но $3 \not\equiv 0 \pmod{6}$ и $4 \not\equiv 0 \pmod{6}$.

103. Использовать утверждение, что если произведение двух чисел делится на простое число p , то хотя бы один из сомножителей делится на p (см. № 155).

105. Целесообразно взять такую полную систему вычетов: $(-3, -2, -1, 0, 1, 2, 3)$.

106. При $a = 3$.

108. а) (1, 2, 3, 4, 5, 6); б) (0, 1, 2, 3, 4, 5); в) $(-3, -2, -1, 0, 1, 2)$ или $(-2, -1, 0, 1, 2, 3)$.

109. 7.

113. 1.

115. а) $x = -1 + 4k$; $y = 2 - 3k$; б) $x = -3 + 8k$; $y = 3 - 7k$.

116. а) Нет решений; б) $x = -6 + 11k$; $y = 5 - 7k$.

117. а) (1; 1), б) (21; 1), (14; 6), (7; 11).

118. Обозначим цифру сотен через x , а цифру десятков через y . Тогда искомое число будет иметь вид: $100x + 10y + 7$. После перенесения цифры 7 на первое

место получим число $700 + 10x + y$. Можем составить уравнение:

$$700 + 10x + y = 2(100x + 10y + 7) + 21.$$

После упрощений получим: $10x + y = 35$.

Но x и y — цифры, значит, единственным решением данного уравнения будет $x = 3$, а $y = 5$. Искомое число равно 357.

119. 72.

120. а) $x = 5 + 7k$; б) нет решений; в) $x = 3 + 5k$.

121. а) $x = 11 + 4k$; $y = 1 + 3k$; б) нет решений.

122. Если цифра десятков x , а цифра единиц y , то уравнение имеет вид: $(10x + y) \cdot 7 = 100x + y$ или $30x - 6y = 0$, откуда $y = 5x$. Так как x и y — цифры, то задача имеет единственное решение $x = 1$; $y = 5$. Искомое двузначное число равно 15.

123. 91.

124. 1 книгу за 3 рубля, 5 книг по 2 рубля и 14 книг по 50 копеек за книгу.

125. НОД $(a, p) = 1$, значит, сравнение имеет единственный класс решений. Подставив значение x в левую часть сравнения, получим: $a \cdot ba^{p-2} = b \cdot a^{p-1} \equiv b \cdot 1 \pmod{p}$, ибо по теореме Ферма $a^{p-1} \equiv 1 \pmod{p}$.

126. Если $a : b$ и $b : a$, то $a = b \cdot q_1$ и $b = a \cdot q_2$, тогда $a = a(q_1q_2)$. Сокращая обе части равенства на a , получим $q_1q_2 = 1$, что возможно лишь при условии, что $q_1 = \pm 1$ и $q_2 = \mp 1$.

127. а) $n + (n + 1) + (n + 2) + (n + 3) + (n + 4) = 5n + 10 = 5(n + 2)$.

б) Любое целое число n может быть представлено в одном из пяти возможных видов: $n = 5k$; $n = 5k + 1$; $n = 5k + 2$; $n = 5k + 3$; $n = 5k + 4$, где k — целое число. Каково бы ни было n , один из сомножителей произведения $n(n + 1)(n + 2)(n + 3)(n + 4)$ делится на 5, а значит, и все произведение делится на 5.

128. Рассматриваем для a пять возможных случаев, как и в предыдущей задаче, предварительно разложив $a^5 - a$ на множители: $a^5 - a = a(a^2 - 1)(a^2 + 1) = (a - 1)a(a + 1) \cdot (a^2 + 1)$.

129. 1) Может, если слагаемых четное число.

2) Нечетное число.

130. Четным. $11 \cdot 10 = 110$.

131. 2) Четным.

132. Число концов у всех мостов должно быть обяза-

тельно четное, а в рукописи имеем $5 + 4 \cdot 4 + 3 \cdot 3 + 1 = 31$ — нечетное число концов.

133. $a + b = 10k$; $a^2 - b^2 = (a + b)(a - b) = 10k(a - b)$.

134. Предположим, что $1970 = a^2 - b^2$, где a и b — целые числа. Значит, $1970 = (a + b)(a - b)$.

В зависимости от четности a и b возможны 4 случая: 1) a и b — оба четные; 2) a и b — оба нечетные; 3) a — четное, b — нечетное; 4) a — нечетное, b — четное. В первых двух случаях $a + b$ и $a - b$ являются четными числами, поэтому их произведение делится на 4. Следовательно, $(a + b)(a - b)$ не может равняться числу 1970, не делящемуся на 4. В последующих двух случаях $a + b$ и $a - b$ — нечетные, значит, их произведение число нечетное и не может равняться четному числу 1970.

135. 1) Да. 2) Не обязательно. 3) Да.

136. 0; 1; 0, 2 или 4; любую цифру от 0 до 7.

137. 1; 1, 3 или 5.

138. 0; любую цифру (0, 1 или 2); 1 или 4; 0, 3 или 6.

139. 0; любую цифру от 0 до 4; 4; 0.

140. 3; 0.

141. 1) 22222222 и другие подобные числа делятся на 9; нет, ибо они на 5 делиться не могут.

2) 555; 555555 и другие подобные числа.

144. Самое большое значение для B будет, если все 1970 цифр числа A равны 9, значит, $B \leq 9 \cdot 1970 = 17\,730$ — пятизначное число. Тогда сумма цифр числа B меньше, чем $9 \cdot 5 = 45$, причем делится на 9. Следовательно, число B может быть 9, 18, 27 или 36. У всех этих чисел сумма цифр равна 9.

145. Исходное и вновь полученное число имеют одинаковое число цифр, ибо мы только переставляем цифру с одного места на другое. Но если при увеличении числа в 5 раз число цифр не изменяется, значит, первая цифра у такого числа равна 1. Число, оканчивающееся на 1, не может делиться на 5.

146. Искомое число обязательно двузначное. Если цифру единиц принять за одну часть, то разность искомого числа и цифры его единиц, оканчивающаяся на нуль, содержит 6 таких частей. Единственное число, оканчивающееся на нуль, которое при делении на 6 дает целое число, меньшее 10, есть число 30. Искомое число 35.

147. $n^4 + 4 = n^4 + 4n^2 + 4 - 4n^2 = (n^2 + 2)^2 - (2n)^2 = (n^2 - 2n + 2)(n^2 + 2n + 2)$.

148. Пусть $n > 1$ — любое натуральное число. Рассмотрим $n - 1$ последовательных натуральных чисел:

$$n! + 2, n! + 3, n! + 4, \dots, n! + n,$$

где $n! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot \dots \cdot n$. Все эти числа составные, ибо $n! + 2$ делится на 2, $n! + 3$ делится на 3 и так далее, наконец, $n! + n$ делится на n . Так как n можно взять сколь угодно большим, то этим и доказано требуемое утверждение.

149. Пусть $\text{НОД}(n + 1, n) = d$, тогда разность $(n + 1) - n = 1$ должна делиться на d , что возможно лишь при $d = 1$.

150. Пусть $\text{НОД}(a, b) = d$, тогда разность $a - b = 2$ обязательно делится на d , значит, $d = 1$ или $d = 2$. Но так как a и b не взаимно простые числа, то $d = 2$.

151. Применим к числам a и b алгоритм Евклида, полагая $a \geq b$. Для определенности будем считать, что процесс последовательного деления закончится на четвертом этапе, то есть

$$a = b \cdot q_1 + r_1,$$

$$b = r_1 \cdot q_2 + r_2,$$

$$r_1 = r_2 \cdot q_3 + r_3,$$

$$r_2 = r_3 \cdot q_4.$$

Тогда $\text{НОД}(a, b) = r_3$. Из предпоследнего равенства найдем $r_3 = r_1 - r_2 \cdot q_3$. Подставим сюда значение r_2 , найденное из второго равенства: $r_2 = b - r_1 q_2$. После упрощений получим: $r_3 = b(-q_3) + r_1(1 + q_2 q_3)$.

Заменим теперь r_1 его выражением из первого равенства: $r_1 = a - b q_1$. После упрощений получим:

$$r_3 = a(1 + q_2 q_3) + b(-q_3 - q_1 - q_1 q_2 q_3).$$

В обеих скобках имеем целые числа, ибо все частные являются целыми числами. Обозначив $1 + q_2 q_3 = x$ и $-q_3 - q_1 - q_1 q_2 q_3 = y$, получим, что $r_3 = \text{НОД}(a, b) = a \cdot x + b \cdot y$.

Очевидно, что таким же рассуждением мы получим требуемое для $\text{НОД}(a, b)$ выражение независимо от того, на каком этапе заканчивается процесс деления.

152. Если a и b взаимно простые числа, то $\text{НОД}(a, b) = 1$, и по доказанному в задаче № 151 найдутся такие числа x и y , что $a \cdot x + b \cdot y = 1$.

Справедливо и обратное. Пусть при некоторых целых x и y имеет место равенство $a \cdot x + b \cdot y = 1$. Тогда любой

общий делитель d чисел a и b будет делителем числа 1, что возможно лишь при $d = \pm 1$. Следовательно, числа a и b имеют только один положительный общий делитель $d = 1$, то есть НОД $(a, b) = 1$.

153. Так как НОД $(a, p) = 1$, то найдутся такие целые числа x и y , что $a \cdot x + p \cdot y = 1$. Умножив обе части этого равенства на b , получим: $(ab)x + p(by) = b$.

По условию $(ab) : p$ и $p : p$, тогда и $b = (ab)x + p(by)$ должно делиться на p .

154. Неверно, например, $3 \cdot 4$ делится на 6, но ни один из сомножителей не делится на 6.

155. 1) Пусть НОД $(a, p) = d$, значит, $p : d$. Но p — число простое, оно может делиться лишь на 1 и на p . Если $d = p$, то тогда $a : p$; если же $d = 1$, значит, a и p взаимно простые.

2) Если a не делится на p , то, по доказанному выше, НОД $(a, p) = 1$, но тогда b должно делиться на p (см. № 153).

3) Пусть произведение $a_1 a_2 a_3 \dots a_n$ делится на простое число p . Рассматривая данное произведение как произведение только двух сомножителей a_1 и $(a_2 a_3 \dots a_n)$, можем рассуждать так: если a_1 не делится на p , то НОД $(a_1, p) = 1$ (см. № 155₁), но тогда второй сомножитель $(a_2 a_3 \dots a_n)$ должен делиться на p (см. № 153).

Аналогично рассуждая, установим, что если a_2 не делится на p , то $(a_3 \dots a_n)$ должно делиться на p . Продолжая эти рассуждения далее, найдем, что если ни одно из чисел $a_1, a_2, a_3, \dots, a_{n-1}$ не делится на p , то a_n делится на p . Итак, какое-нибудь из данных n чисел обязательно делится на p .

156. Пусть для некоторого числа N мы имеем два разложения: $N = p_1 \cdot p_2 \dots p_k$ и $N = q_1 \cdot q_2 \dots q_s$, где все p_i и q_n — простые числа. Требуется доказать, что числа q_1, q_2, \dots, q_s лишь порядком расположения могут отличаться от чисел p_1, p_2, \dots, p_k .

Рассмотрим равенство: $p_1 \cdot p_2 \dots p_k = q_1 \cdot q_2 \dots q_s$. Левая часть его делится на p_1 , значит, и правая часть должна делиться на p_1 . Но p_1 — число простое, поэтому произведение $q_1 \cdot q_2 \dots q_s$ делится на p_1 только в том случае, когда один из его сомножителей делится на p_1 (см. № 155₃). Пусть q_1 делится на p_1 , но так как q_1 — число простое, значит, $q_1 = p_1$ (см. № 49). Разделив обе части равенства на p_1 , получим: $p_2 \cdot p_3 \dots p_k = q_2 \cdot q_3 \dots q_s$.

Аналогично найдем, что $q_2 = p_2$; $q_3 = p_3$ и так далее. Получим, что все множители p_1, p_2, \dots, p_k входят и в правую часть исходного равенства.

Рассматривая делимость на q , получим, что все множители q_1, q_2, \dots, q_s входят в левую часть. Следовательно, левая и правая части могут отличаться только порядком множителей, а не самими множителями.

157. Так как $a : p$, то $a = p \cdot Q$; но $a : q$, значит, $(p \cdot Q) : q$. По условию НОД $(p, q) = 1$, поэтому $Q : q$ (см. № 153), то есть $Q = q \cdot c$. Тогда $a = p \cdot q \cdot c$.

158. Так как $6 = 2 \cdot 3$, $12 = 3 \cdot 4$ и $15 = 3 \cdot 5$ представлены в виде произведений взаимно простых чисел, можно сформулировать следующие признаки делимости:

на 6 делятся те и только те числа, которые делятся и на 2, и на 3;

на 12 делятся те и только те числа, которые делятся и на 3, и на 4;

на 15 делятся те и только те числа, которые делятся и на 3, и на 5.

159. 1) Произведение трех последовательных чисел делится и на 2, и на 3 (см. № 18), значит, оно делится и на 6.

2) Произведение четырех последовательных целых чисел делится на 3 (см. № 18). Среди сомножителей обязательно есть два четных числа: $2k$ и $2k + 2$. Их произведение делится на 8, ибо $2k \cdot (2k + 2) = 4k(k + 1)$, а $k(k + 1)$ делится еще на 2 (см. № 18). Значит, все произведение делится на 24, так как НОД $(3, 8) = 1$.

3) Произведение $n(n + 1)(n + 2)(n + 3)(n + 4)$ делится на 3, на 8 и на 5, следовательно, и на $3 \cdot 5 \cdot 8 = 120$.

160. 1) $a^3 - a = a(a^2 - 1) = (a - 1)a(a + 1)$.

2) $a^5 - a = a(a^2 - 1)(a^2 + 1) = (a - 1)a(a + 1)(a^2 + 1)$; при любом целом a это произведение делится на 2, на 3 и на 5 (см. № 128).

3) Как и при решении задачи № 18, устанавливаем делимость на 2 и на 3.

4) $a^5 - 5a^3 + 4a = a(a^2 - 1)(a^2 - 4) = (a - 2)(a - 1) \times \times a(a + 1)(a + 2)$. Получили произведение пяти последовательных целых чисел.

$$5) \frac{a}{3} + \frac{a^2}{2} + \frac{a^3}{6} = \frac{2a + 3a^2 + a^3}{6} = \frac{a(a + 1)(a + 2)}{6}.$$

В числителе получили произведение трех последовательных целых чисел, которое делится на 6.

$$6) \frac{a^4}{24} + \frac{a^3}{4} + \frac{11a^2}{24} + \frac{a}{4} = \frac{a^4 + 6a^3 + 11a^2 + 6a}{24} =$$

$= \frac{a(a+1)(a+2)(a+3)}{24}$. В числителе имеем произведение четырех последовательных целых чисел, которое делится на 24.

161. Пусть M — общее кратное чисел a и b . $m = \text{НОК}(a, b)$. Разделим M на m .

$$M = m \cdot q + r, \text{ где } 0 \leq r < m.$$

Так как M делится и на a и на b , и m делится и на a и на b , то и r должно делиться и на a и на b , то есть r есть общее кратное чисел a и b . Но наименьшим положительным общим кратным чисел a и b является m , значит, $r = 0$.

162. Если делитель $d = 1$, то его можно представить в виде $p_1^0 \cdot p_2^0 \cdot \dots \cdot p_n^0$. Если $d > 1$, то он имеет простой делитель p . Так как $N : d$ и $d : p$, то $N : p$, значит, один из простых множителей разложения N должен делиться на p , что возможно, если он совпадает с p , иными словами, p есть один из p_i , входящих в каноническое разложение числа N .

Если некоторое простое число p входит в разложение числа N в степени α , а в разложение d в степени β , то $\beta \leq \alpha$. Предположим противное, что $\beta > \alpha$. Тогда $N = p^\alpha \cdot q_1$, причем q_1 не делится на p , а $d = p^\beta q_2$.

По условию $N : d$, значит, $N = d \cdot q_3 = p^\beta q_2 q_3$. Составим равенство: $p^\alpha q_1 = p^\beta q_2 q_3$. Сократив на p^α , получим $q_1 = p^{\beta-\alpha} q_2 q_3$. Правая часть делится на p , а левая не делится. Полученное противоречие и доказывает, что β не может быть больше α .

163. Число делителей равно $(\alpha_1 + 1)(\alpha_2 + 1) \cdot \dots \cdot (\alpha_n + 1)$.

165. Остаток равен 5.

166. 1) $3 \cdot 7 + 2 = 23$. 2) $60 \cdot n + 1 = 301$.

167. 1) 4; 4. 2) 25 или 70 и 40 или 85.

168. 1) 3420; 4320; 3240; 2340. 2) Нельзя.

169. 167.

170. Так как $5^6 \equiv 1 \pmod{7}$, достаточно найти остаток

от деления числа $7^{\overbrace{7}^{\cdot 7}}$ на 6. Но $7 \equiv 1 \pmod{6}$, поэтому

$$7 \overline{7} \equiv 1 \pmod{6}, \quad \text{значит,} \quad 5 \overline{7} \equiv 5^{6n+1} = (5^6)^n \cdot 5 \equiv 5 \pmod{7}.$$

171. По модулю 7 имеем:

$$\text{а) } 222^{555} + 555^{222} \equiv 5^{555} + 2^{222} = 5^{6 \cdot 92 + 3} + 2^{6 \cdot 37} \equiv 5^3 + 1 \equiv 0.$$

$$\text{б) } 2222^{5555} + 5555^{2222} \equiv 3^{5555} + 4^{2222} = 3^{6 \cdot 925 + 5} + 4^{6 \cdot 370 + 2} \equiv 3^5 + 4^2 \equiv 5 + 2 \equiv 0.$$

172. Пусть $p-1 = kq + r$, где $0 < r < k$, тогда $a^{p-1} = a^{kq+r} = (a^k)^q \cdot a^r$. Но $a^k \equiv 1 \pmod{p}$ и $a^{p-1} \equiv 1 \pmod{p}$, значит, $1 \equiv 1 \cdot a^r \pmod{p}$, чего быть не может, ибо $0 < r < k$, а по условию k — наименьшее натуральное число такое, что $a^k \equiv 1 \pmod{p}$.

173. Когда x пробегает все $\varphi(m)$ значений из приведенной системы вычетов, получим $\varphi(m)$ произведений ax , и так как a и x взаимно просты с m , то и их произведения взаимно просты с m . Нетрудно показать, что все $\varphi(m)$ произведений принадлежат разным классам вычетов по модулю m .

174. Возьмем любую приведенную систему вычетов r_1, r_2, \dots, r_s , где $s = \varphi(m)$. Тогда числа ar_1, ar_2, \dots, ar_s также образуют приведенную систему вычетов по тому же модулю m . Поэтому каждое из чисел ar_k сравним по модулю m с одним из чисел r_i , а перемножив все $s = \varphi(m)$ этих сравнений, получим:

$$a^{\varphi(m)} \cdot r_1 r_2 \cdot \dots \cdot r_s \equiv r_1 r_2 \cdot \dots \cdot r_s \pmod{m}.$$

Но все r_i взаимно просты с m , тогда и их произведение $r_1 r_2 \cdot \dots \cdot r_s$ взаимно просто с m . Разделив обе части сравнения на это произведение, получим: $a^{\varphi(m)} \equiv 1 \pmod{m}$.

175. Сравнение $127^{107} \equiv 7^{107} \pmod{15}$ очевидно. Непосредственно определяем, что числа 1, 2, 4, 7, 8, 11, 13, 14 образуют приведенную систему вычетов по модулю 15, значит, $\varphi(15) = 8$. По теореме Эйлера $7^8 \equiv 1 \pmod{15}$, тогда $7^{107} = 7^{8 \cdot 13 + 3} = (7^8)^{13} \cdot 7^3 \equiv 7^3 \pmod{15}$. Теперь находим остаток: $7^3 = 49 \cdot 7 \equiv 4 \cdot 7 \equiv 13 \pmod{15}$.

176. а) $x = 2 + 12k$; $y = 3 - 11k$; б) $x = 1 + 2k$; $y = 3 + 9k$.

177. 198.

178. Обозначим искомые цифры через x , y и z , причем будем считать, что $x < y < z$. Из этих трех букв можно составить только шесть различных групп по три буквы: $x y z$; $x z y$; $y x z$; $y z x$; $z x y$ и $z y x$. Поэтому комбинируя три цифры, мы получим шесть трехзначных чисел, в общую сумму которых каждая буква входит дважды в качестве цифры сотен, дважды — десятков и дважды — единиц. Следовательно, $(200 + 20 + 2)x + 222y + 222z = 2886$, откуда $x + y + z = 13$.

С другой стороны, $(100z + 10y + x) - (100x + 10y + z) = 495$; $99z - 99x = 495$; $z - x = 5$.

Если $x = 1$, тогда $z = 6$ и $y = 6$, чего быть не может, ибо все цифры разные. Если $x \geq 3$, тогда $z \geq 8$, а $y \leq 2$ что противоречит условию $x < y < z$.

Следовательно, $x = 2$; $z = 7$ и $y = 4$.

179. Столов с одним ящиком было 5, с двумя — 3, с тремя — 2 и с четырьмя — 4.

180. Пусть было x пятерок и y рублей, значит, всего было $(5x + y)$ рублей, а после покупок осталось $(5y + x)$ рублей. Из уравнения $5x + y = 3(5y + x)$ находим: $2x = 14y$ или $x = 7y$. Следовательно, первоначальная сумма составляла $5 \cdot 7y + y = 36y$ рублей, что немного меньше 150 рублей только при $y = 4$. Значит, до покупок у них было 144 рубля, осталось 48 рублей, а на покупки израсходовали 96 рублей.

181. Обозначим число восьмиклассников через n , а число очков, полученных каждым из них, через x . Так как за каждую партию начисляется либо 1 очко одному, либо по 0,5 очка каждому, то число $2x$ должно быть целым.

Всего участников было $n + 2$, значит, ими было сыграно $\frac{(n+2)(n+1)}{2}$ партий и столько же всего было начислено

очков. Составляем уравнение: $\frac{(n+2)(n+1)}{2} = n \cdot x + 8$.

$$n^2 + 3n + 2 = 2nx + 16; 2nx = n^2 + 3n - 14, \text{ откуда}$$

$$2x = n + 3 - \frac{14}{n}.$$

Но n и $2x$ — числа целые, поэтому n должно быть положительным делителем числа 14. Но при $n = 1$ и $n = 2$ получим, что $2x < 0$, что быть не может. При $n = 7$ получим $x = 4$, а при $n = 14$ будет $x = 8$. Таким образом, в турнире участвовало или 7, или 14 восьмиклассников,

ЛИТЕРАТУРА

А. И. Маркушевич. Дополнительные вопросы арифметики целых чисел. «Математика в школе», № 4, 1967.

А. Я. Хинчин. Элементы теории чисел. Энциклопедия элементарной математики, т. I.

М. К. Гребенча и С. Е. Ляпин. Арифметика. Учпедгиз, М., 1952.

Н. Н. Воробьев. Признаки делимости. Физматиздат, М., 1963.

В. Серпинский. Что мы знаем и чего не знаем о простых числах. Физматиздат, М., 1963.

Алексей Архипович Мазаник

ДЕЛИМОСТЬ ЧИСЕЛ И СРАВНЕНИЯ

Редактор Б. А. Кимбар. Художественный редактор И. Я. Карпинovich.

Технический редактор М. Т. Попкова. Корректор Л. С. Калиновская.

Сдано в набор 5/VIII 1970 г. Подписано к печати 4/XI 1970 г. Формат 84×108¹/₃₂.

Бум. тип. № 3. Физ. печ. л. 2. Усл. печ. л. 3,36. Уч.-изд. л. 3,23. Тираж 40 000 экз.

Зак. 1151. Цена 9 коп.

Издательство «Народная асвета» Государственного комитета
Совета Министров БССР по печати, Минск, Ленинский проспект, 85.

Типография издательства ЦК КП Белоруссия, Минск, Ленинский проспект, 79

9 коп.