А. И. Сгибнев

Делимость чисел и простые числа

Издательство МЦНМО
Москва, 2012

Предисловие

При изложении курса «Делимость чисел и простые числа» есть два основных подхода. Первый ставит во главу угла логику изложения: все утверждения доказываются, а недоказанные не используются. См., например, [1]. Второй делает упор на задачах: основная теорема арифметики формулируется сразу и без доказательства, что позволяет не заниматься теоретическими тонкостями, а сразу же решать содержательные задачи. См., например, [2].

Я попытался пойти средним путём. Мне кажется принципиально важным в математическом курсе доказывать (раньше или позже) все утверждения. Однако без задачного подкрепления доказательства теорем часто превращаются в формальные тексты. Например, чего стоит для восьмиклассника данное без подготовки утверждение:

«Для любых взаимно простых a и b найдутся такие x и y, что $ax + by = 1$»!

Поэтому этапы доказательств растянулись на несколько занятий, в которых используемые идеи и конструкции мотивируются и используются в задачах. Кроме того, иногда я позволял себе брать утверждения «взаймы», жертвуя последовательностью изложения ради его живости[1].

В результате (как я надеюсь) этапы доказательств стали доступны, а по ходу решаются интересные задачи. Правда, в ходе «размазывания» этапов затемнилась логическая структура доказательства основной теоремы ариф-

[1] А именно, в занятии 2 формулируется теорема о взаимно простых делителях, которая используется при решении задач на признаки делимости; в занятии 6 приводится теорема о сокращении простого множителя, нужная для решения неоднородных диофантовых уравнений.

метики. Приведём краткую схему для учителя и подготовленного ученика:

1. Вводится понятие простого числа и доказывается, что любое число раскладывается на простые множители; при этом вопрос однозначности не изучается (занятие 4).

2. Вводится алгоритм Евклида (занятие 5).

3. С помощью алгоритма Евклида доказывается основная лемма (занятие 6).

4. Из основной леммы выводится теорема о простом делителе (занятие 7).

5. Из теоремы о простом делителе выводится однозначность разложения на простые множители (занятие 8).

Также в занятии 6 из основной леммы выводятся теоремы о взаимно простых делителях и о сокращении множителя (но в минимальной логической схеме они необязательны).

Теоремам о делимости даны названия, чтобы школьникам было легче «узнавать их в лицо».

При решении задач из первых занятий у школьников, возможно, будет возникать соблазн ссылаться на ещё не доказанные свойства простых чисел, однозначность разложения на простые множители и т. д. Однако все задачи можно решить, опираясь на доказанный материал в рамках того занятия, на котором они даются. Полезно требовать от школьников делать это, приучая их к «чистоте» решения.

Подавляющее большинство задач не придумано автором, а взято из литературы (зачастую с некоторыми изменениями в формулировках). Книга [1] повлияла на логическую структуру курса (доказательство основной теоремы арифметики). Книга [2] дала многие идеи задач и задачных циклов. Из книги [3] взято много ярких формулировок (особенно задач на диофантовы уравнения).

Автор благодарен А. Д. Блинкову, И. Б. Писаренко и своим ученикам. Особенную признательность автор выражает А. В. Шаповалову, помощь которого заметно превышала обычные для редактора рамки.

Занятия 1–4 ориентированы на 7–8 класс, занятия 5–7 — на 8–9 класс.

Наиболее важные задачи помечены знаком «+», наиболее сложные задачи — знаком «*». Если не оговорено противное, под «числами» понимаются «целые числа».

Занятие 1

Делимость чисел

Определение. Говорят, что число a делится на число b (или a кратно b), если найдётся такое целое число q, что $a = b \cdot q$. Обозначение: $a \vdots b$.

Наглядная интерпретация: если a монет можно разложить на b одинаковых стопок, то a кратно b. Другая интерпретация: если a монет можно разложить на несколько кучек по b монет в каждой, то a кратно b. Из нее следует, что на пары разбивается только чётное число.

Заметим, что если $a \vdots b$, то $a \vdots (-b)$ (докажите!). Поэтому, если не оговорено противное, мы будем искать только *положительные делители* чисел.

Задача 1.1. Найдите все делители числа 36.

Решение. Будем последовательно проверять числа 1, 2, 3, 4 и т. д.: если их произведение на какое-то число даст 36, запишем это: $36 = 1 \cdot 36 = 2 \cdot 18 = 3 \cdot 12 = 4 \cdot 9 = 6 \cdot 6 = 9 \cdot 4 = 12 \cdot 3 = 18 \cdot 2 = 36 \cdot 1$.

Заметим, что в записи $a = bq$ оба числа b и q являются делителями числа a. Поэтому перебор можно остановить на произведении $6 \cdot 6$.

Задача 1.2.[+] В верхней строке таблицы указано то, что **дано.** В левом столбце — то, что **спрашивается.** Заполните пустые клетки: если «да», то поставьте «+», если «нет», то «$-$», если данных не хватает, то знак «?». Обоснуйте свои ответы.

	$a \vdots m$ и $b \vdots m$	$a \vdots m$ и $b \not\vdots m$	$a \not\vdots m$ и $b \not\vdots m$
$a + b \vdots m$?			
$a - b \vdots m$?			
$a \cdot b \vdots m$?			

Решение. Рассмотрим первую строку таблицы. Так как $a = km$ и $b = lm$, то $a + b = (k + l)m$, то есть $a + b$ делится на m. С клеткой под ней (разность) всё аналогично. Возможно и такое рассуждение: поскольку $b \,\vdots\, m$, то и $-b \,\vdots\, m$, следовательно, и сумма $a + (-b)$ делится на m.

Теперь рассмотрим третью клетку в первой строке. $5 \not\vdots\, 3$ и $1 \not\vdots\, 3$, но $5 + 1 \,\vdots\, 3$. Однако $5 \not\vdots\, 3$ и $2 \not\vdots\, 3$ и также $5 + 2 \not\vdots\, 3$. Поэтому данных недостаточно. Аналогичные примеры можно привести и для разности.

Рассмотрим вторую клетку в первой строке. Предположим, что $c = a + b \,\vdots\, m$. Тогда и $b = c - a$ должно делиться на m как разность двух чисел, делящихся на m. Полученное противоречие показывает, что $a + b$ не делится на m. Аналогично и с разностью.

Теперь рассмотрим делимость произведения (третья строка). Поскольку $a = km$, то $ab = (kb)m \,\vdots\, m$ независимо от делимости b на m.

В последней клетке третьей строки ab может не делиться на m (например $a = b = 1$, $m = 2$), но может и делиться (например, $a = b = 2$, $m = 4$). Значит, данных не хватает.

Можно дать наглядную интерпретацию большинству ответов: если каждая из двух кучек монет раскладывается на стопки по m монет, то и объединённая кучка тоже разложится, и т. д.

Результаты этой задачи полезно запомнить:

	$a \,\vdots\, m$ и $b \,\vdots\, m$	$a \,\vdots\, m$ и $b \not\vdots\, m$	$a \not\vdots\, m$ и $b \not\vdots\, m$
$a + b \,\vdots\, m$?	+	–	?
$a - b \,\vdots\, m$?	+	–	?
$a \cdot b \,\vdots\, m$?	+	+	?

Обратите внимание учеников на то, что в первой и второй строчках ответы одинаковы (в этом смысле сумма и разность с точки зрения делимости неразличимы). На занятии 7 мы поймём, от чего зависит делимость чисел в третьем столбце.

Задача 1.3. Определите, не выполняя действий, делится ли а) $18^2 - 7^2$ на 11; б) $53^3 + 67^3 + 2^3$ на 60; в) $1^3 + 2^3 + \ldots + 82^3$ на 83.

Решение. а) Делится: $18^2-7^2=(18-7)(18+7)=11\cdot25\ \vdots$ $\vdots\ 11$.

б) Не делится: $53^3+67^3=(53+67)(53^2-53\cdot67+67^2)=$ $=120(53^2-53\cdot67+67^2)\ \vdots\ 60$, а $2^3 \not\vdots\ 60$.

в) Делится: разобьём слагаемые на пары и докажем, что сумма в каждой паре делится на 83. Например, 1^3+ $+82^3\ \vdots\ 83$, $2^3+81^3\ \vdots\ 83$.

Задача 1.4. Петя считает, что если a^2 делится на $a-b$, то b^2 делится на $a-b$. Прав ли он?

Решение. Рассмотрим разность двух Петиных выражений: $a^2-b^2=(a-b)(a+b)\ \vdots\ (a-b)$. Поскольку уменьшаемое и разность делятся на $a-b$, то по задаче 1.2 и вычитаемое должно делиться на $a-b$. Поэтому Петя прав.

Может быть полезна такая формулировка: если сумма (разность) двух чисел делится на m, то либо оба числа делятся на m, либо оба не делятся.

Задача 1.5. а) Докажите, что квадрат натурального числа имеет нечётное количество делителей. б) Верно ли обратное?

Решение. а) Сгруппируем делители числа $n=m^2$: если d — делитель числа n, то $\frac{n}{d}$ — тоже делитель; объединим их в пару. Только m попадёт в пару с самими собой, а все остальные делители n разобьются на пары. Поэтому у квадрата нечётное число делителей.

б) Если количество делителей нечётно, значит, есть пара совпадающих делителей. Следовательно, число является квадратом, то есть обратное также верно.

Задача 1.6. Докажите, что а) произведение двух последовательных чисел делится на 2; б) число $\frac{n^2+n}{2}$ — целое.

Решение. а) Заметим, что среди двух подряд идущих чисел хотя бы одно делится на 2. По задаче 1.2 произведение также делится на 2.

б) Разложим числитель на множители: $n^2+n=n(n+1)$. Получим произведение двух последовательных чисел, которое чётно по п. а).

Задачи для самостоятельного решения

Задача 1.7. В каком случае два числа a и b таковы, что a делится на b и b делится на a?

Задача 1.8^{+}. а) Верно ли, что если $a \vdots m$ и $b \vdots n$, то $ab \vdots mn$? б) Верно ли, что если $a \vdots b$ и $b \vdots c$, то $a \vdots c$?

Задача 1.9. Вася считает, что если $ab + cd$ делится на $a - c$, то $ad + bc$ тоже делится на $a - c$. Прав ли он?

Задача 1.10. В Тройном королевстве имеют хождение только монеты по 9 и по 15 золотых. Докажите, что такими монетами нельзя набрать сумму в 50 золотых.

Задача 1.11. а) Маша показывает такой фокус: ей называют любое трёхзначное число, она приписывает к нему такое же, а потом в уме за секунду делит получившееся шестизначное число на 1001. Как она это делает?

б) Саша заметила, что все шестизначные числа Маши делятся на 7. Почему? На какие ещё числа они делятся?

Задача 1.12. В некотором государстве была тюрьма, в каждой из ста камер которой сидело по одному заключённому. Камеры были пронумерованы числами от 1 до 100, а замки в них были устроены так, что при одном повороте ключа дверь открывалась, при следующем повороте — закрывалась и т. д. Царь в то время воевал с соседним государством, и в какой-то момент ему показалось, что он побеждает.

На радостях царь послал гонца с указанием отпереть все камеры, но затем ход военных действий изменился, и царь послал другого гонца вдогонку первому, наказав ему повернуть ключ в замке в каждой второй камере; затем был послан следующий гонец, чтобы повернуть ключ в замке у каждой третьей камеры, и т. д.

Таким образом 100 гонцов прибывали в тюрьму один за другим и последовательно поворачивали замки в камерах. Сколько узников в итоге вышло на свободу и из каких камер?

Ответы и решения

Задача 1.7. Из того, что a делится на b, следует, что $|a| \geqslant |b|$. Из того, что b делится на a, следует, что $|b| \geqslant |a|$. Два неравенства вместе дают $|a| = |b|$, то есть числа могут отличаться только знаками.

Задача 1.8. а) Верно: так как $a = lm$, а $b = kn$, то $ab = (kl)(mn)$, то есть по определению делится на mn.

б) Верно: так как $a = kb$, $b = lc$, то $a = (kl)c$, то есть по определению a делится на c.

Эти упражнения достаточно простые, однако важно, чтобы школьники привыкли корректно доказывать утверждения, ссылаясь на определение. Скажем, в предыдущем упражнении полезнее говорить «произведение кратно mn», чем «в частном будет целое число».

Задача 1.9. Действуя аналогично задаче 1.4, найдём разность двух выражений: $(ab + cd) - (ad + bc) = a(b - d) - c(b - d) = (a - c)(b - d) \vdots (a - c)$. Поэтому и второе выражение делится на $a - c$.

Задача 1.10. Заметим, что 9 и 15 делятся на 3, поэтому любая сумма, набранная такими монетами, также делится на 3. Однако 50 не делится на 3.

Задача 1.11. а) Заметим, что $\overline{abcabc} = 1001\overline{abc}$. Поэтому частное просто равно исходному числу.

б) $1001 = 7 \cdot 11 \cdot 13$, поэтому числа вида $\overline{abcabc}$ делятся на 7, на 11, на 13 и на их попарные произведения.

Задача 1.12. Заметим, что на свободу вышли узники из тех и только тех камер, в которых ключ повернули нечётное количество раз, то есть номера которых имеют нечётное количество делителей. По задаче 1.5 это квадраты, то есть искомые номера: 1, 4, 9, 16, ..., 100. Всего их десять.

К теме данного занятия относятся также задачи 1–7 из раздела «Дополнительные задачи».

Приложение

Две ещё не решённые задачи о простых числах

В теории чисел встречаются задачи с очень простой формулировкой, решения которых до сих пор неизвестны. Школьников полезно знакомить с такими задачами — в частности для того, чтобы избавить их от иллюзии, что «в математике уже всё открыто».

1. Гольдбах заметил, что любое чётное число (кроме 2) удаётся представить в виде суммы двух простых чисел. Например, $4 = 2 + 2$, $6 = 3 + 3$, $8 = 5 + 3$, $10 = 5 + 5$, $12 = 5+7$, $14 = 7+7$, $16 = 13+3$, $18 = 11+7$, ..., $100 = 97+3$ и т. д. Гипотеза Гольдбаха до сих пор не доказана. Можно изучать экспериментально (с помощью компьютера) количество представлений числа $2n$ в виде суммы двух простых чисел.

2. Простые числа нередко встречаются парами в виде p и $p + 2$. Таковы 3 и 5, 11 и 13, 29 и 31 и т. д. Бесконечно ли множество таких «близнецов»?

Несколько исследовательских задач, связанных с делимостью

Разрешимость линейных уравнений в неотрицательных целых числах

Основная лемма гарантирует, что выражение $ax + by$ при данных взаимно простых a и b может принять любое целое значение при надлежащем выборе целых x и y. Интересно посмотреть, что будет, если ограничиться целыми неотрицательными x и y. Например, в задаче 6.10

доказано, что уравнение $3x + 5y = N$ разрешимо в неотрицательных целых числах при всех $N > 7$. Обобщим задачу. *Даны взаимно простые a и b; при каких N разрешимо уравнение $ax + by = N$?* Удобно организовать исследование так: зафиксировав a и b, отмечать на целочисленной оси зелёным цветом все числа, представимые в виде $ax + by$, а красным — непредставимые, и искать закономерности.

Нетрудно заметить, что уравнение неразрешимо лишь для конечного количества правых частей, то есть всегда найдётся такое граничное число N_0, что все бóльшие числа выражаются в виде $ax + by$ (как и в частном случае задачи **6.10**, где $N_0 = 7$). Чтобы угадать зависимость N_0 от a и b, можно зафиксировать a и находить граничное число, последовательно увеличивая b. (Ясно, что a и b должны входить в формулу симметрично.) Далее достаточно доказать, что N_0 непредставимо в виде $ax + by$, а все $N > N_0$ представимы.

Красивую закономерность (и идею решения) можно увидеть, если посмотреть на размеченную числовую ось геометрически. См. А. В. Спивак. *Арифметика.* М.: Бюро Квантум, 2007. С. 30–32.

Квадратичные вычеты

Остатки от деления квадратов натуральных чисел на число M называются *квадратичными вычетами* числа M. Остальные числа в пределах от 0 до $M - 1$ называются *квадратичными невычетами* числа M. Например, числа 0 и 1 являются квадратичными вычетами числа 3, а число 2 — квадратичным невычетом.

а) Найдите все квадратичные вычеты для чисел $M = 2$, 5, 7, 11. Что можно сказать про их количество?

б) Сформулируйте гипотезу для всех простых $M > 2$ и докажите её.

в*) Проделайте то же для M, равного произведению различных простых чисел.

г**) Решите ту же задачу для произвольного M.

См. В. В. Острик, М. А. Цфасман. *Алгебраическая геометрия и теория чисел: рациональные и эллиптические кривые.* М.: МЦНМО, 2005. С. 11, 41, 42.

Первообразные корни

Возьмём простое число, например $p = 7$, и будем искать остатки от деления степеней 2 на 7:

2 даёт остаток 2, 2^2 даёт остаток 4, 2^3 даёт остаток 1, 2^4 даёт остаток 2, ...

Теперь посмотрим на остатки от деления степеней 3 на 7:

3 даёт остаток 3, 3^2 даёт остаток 2, 3^3 даёт остаток 6, 3^4 даёт остаток 4, 3^5 даёт остаток 5, 3^6 даёт остаток 1, ...

Нетрудно понять, что последовательность рано или поздно зациклится. Для $a = 3$ остатки успели пробежать все возможные числа $1, 2, \ldots, p-1$. В этом случае число a называют первообразным корнем по модулю p. Для $a = 2$ цикл состоит всего из трёх чисел.

Возникают вопросы:

а) У любого ли простого p есть первообразный корень?

б) Какую длину может иметь цикл степеней числа a по модулю p?

в) Каково количество первообразных корней для данного простого p?

Разумно продолжить эксперимент: выбираем простое p и рассматриваем последовательно степени $a = 2, 3, \ldots p-2$ (для $a = 1$, $p-1$ всё понятно). Гипотезы и доказательство п. б) найти несложно, а вот доказательство п. а) весьма трудно.

Пасхалия

Один из главных праздников христиан — Пасха — является переходящим, то есть в каждый год выпадает на новую дату. Православные празднуют Пасху в первое воскресенье после первого полнолуния, бывшего после

21 марта[2]. Важность знания даты Пасхи в средние века показывает, например, шотландская сказка, в которой жители Шотландии каждый год отправляли гонца в Ватикан, чтобы узнать дату очередной Пасхи. Герой сказки прославился тем, что смог узнать не только дату, но и сам способ вычисления.

Гаусс нашёл простой алгоритм вычисления дня православной Пасхи, который записывается в несколько строк. Обозначим через a остаток от деления числа года на 19, через b — остаток от деления его на 4 и через c — от деления на 7. Далее, остаток от деления величины $19a + 15$ на 30 назовем d, а остаток от деления $2b + 4c + 6d + 6$ на 7 пусть будет e. День Пасхи будет $22 + d + e$ марта, или, что то же самое, $d + e - 9$ апреля (по юлианскому календарю!).

По этому алгоритму можно сделать небольшую исследовательскую работу, руководствуясь следующим планом.

а) Периодична ли дата Пасхи? Найдите период (он называется великий индиктион).

б) Проверьте, что в 2010 году была самая ранняя Пасха. Когда будет следующая самая ранняя Пасха? Когда будет ближайшая самая поздняя Пасха? Сколько раз за период они встречаются?

в) Все ли промежуточные даты встречаются? Какие даты встречаются чаще всего, какие — реже всего?

г) Может ли одна и та же дата Пасхи выпадать два года подряд?

д*) (для любителей астрономии). Докажите алгоритм Гаусса.

Можно с помощью компьютера составить вечную пасхалию, то есть даты Пасхи на полный период.

[2]По юлианскому календарю, отстающему сейчас на 13 дней от григорианского, по которому мы живём.

Раздаточный материал

Занятие 1. Делимость чисел

Задача 1.1. Найдите все делители числа 36.

Задача 1.2$^+$. В верхней строке таблицы указано то, что **дано.** В левом столбце — то, что **спрашивается.** Заполните пустые клетки: если «да», то поставьте «+», если «нет», то «–», если данных не хватает, то знак «?». Обоснуйте свои ответы.

	$a \vdots m$ и $b \vdots m$	$a \vdots m$ и $b \not\vdots\, m$	$a \not\vdots\, m$ и $b \not\vdots\, m$
$a + b \vdots m$?			
$a - b \vdots m$?			
$a \cdot b \vdots m$?			

Задача 1.3. Определите, не выполняя действий, делится ли
а) $18^2 - 7^2$ на 11;
б) $53^3 + 67^3 + 2^3$ на 60;
в) $1^3 + 2^3 + \ldots + 82^3$ на 83.

Задача 1.4. Петя считает, что если a^2 делится на $a - b$, то b^2 делится на $a - b$. Прав ли он?

Задача 1.5. а) Докажите, что квадрат натурального числа имеет нечётное количество делителей.

б) Верно ли обратное?

Задача 1.6. Докажите, что:
а) произведение двух последовательных чисел делится на 2;
б) число $\dfrac{n^2 + n}{2}$ — целое.

Задача 1.7. В каком случае два числа a и b таковы, что a делится на b и b делится на a?

Задача 1.8$^+$. а) Верно ли, что если $a \vdots m$ и $b \vdots n$, то $ab \vdots mn$?

б) Верно ли, что если $a \vdots b$ и $b \vdots c$, то $a \vdots c$?

Задача 1.9. Вася считает, что если $ab + cd$ делится на $a - c$, то $ad + bc$ тоже делится на $a - c$. Прав ли он?

Задача 1.10. В Тройном королевстве имеют хождение только монеты по 9 и по 15 золотых. Докажите, что такими монетами нельзя набрать сумму в 50 золотых.

Задача 1.11. а) Маша показывает такой фокус: ей называют любое трёхзначное число, она приписывает к нему такое же, а потом в уме за секунду делит получившееся шестизначное число на 1001. Как она это делает?

б) Саша заметила, что все шестизначные числа Маши делятся на 7. Почему? На какие ещё числа они делятся?

Задача 1.12. В некотором государстве была тюрьма, в каждой из ста камер которой сидело по одному заключённому. Камеры были пронумерованы числами от 1 до 100, а замки в них были устроены так, что при одном повороте ключа дверь открывалась, при следующем повороте — закрывалась и т. д. Царь в то время воевал с соседним государством, и в какой-то момент ему показалось, что он побеждает.

На радостях царь послал гонца с указанием отпереть все камеры, но затем ход военных действий изменился, и царь послал другого гонца вдогонку первому, наказав ему повернуть ключ в замке в каждой второй камере; затем был послан следующий гонец, чтобы повернуть ключ в замке у каждой третьей камеры и т. д.

Таким образом 100 гонцов прибывали в тюрьму один за другим и последовательно поворачивали замки в камерах. Сколько узников в итоге вышло на свободу и из каких камер?

Список литературы и веб-ресурсов

1. В. Г. Болтянский, Г. Г. Левитас. *Делимость чисел и простые числа.* // В книге: *Дополнительные главы по курсу математики. Учебное пособие по факультативному курсу для учащихся 7–8 классов.* М.: Просвещение, 1974.

2. Н. Б. Васильев, В. Л. Гутенмахер, Ж. М. Раббот, А. Л. Тоом. *Заочные математические олимпиады.* — М.: Наука, 1986.

3. Н. Н. Воробьёв. *Признаки делимости.* — М.: Наука, 1988.

4. Е. В. Галкин. *Нестандартные задачи по математике. Задачи с целыми числами.* Челябинск: Взгляд, 2005.

5. С. А. Генкин и др. *Ленинградские математические кружки.* Киров: АСА, 1994.

6. *Задачи по математике, предлагавшиеся ученикам математического класса* 57 *школы* (*выпуск* 2000 *года, класс «В»*) // Под ред. А. Шеня. — М.: МЦНМО, 2000.

7. *Задачи по математике, предлагавшиеся ученикам математического класса* 57 *школы* (*выпуск* 2004 *года, класс «Д»*) // Под ред. В. Доценко. — М.: МЦНМО, 2004.

8. Л. И. Звавич, А. Р. Рязановский. *Алгебра.* 8 *кл.*: *Задачник для кл. с углуб. изуч. математики.* — М.: Мнемозина, 2002.

9. Р. Курант, Г. Роббинс. *Что такое математика*? М.: МЦНМО, 2004.

10. *Московские математические регаты.* Составители А. Д. Блинков, Е. С. Горская, В. М. Гуровиц. — М.: МЦНМО, 2007.

11. А. В. Спивак. *Арифметика.* — М.: Бюро Квантум, 2007.

12. А. Шень. *Простые и составные числа.* М.: МЦНМО, 2005.

Список веб-ресурсов

1. `http://problems.ru/` — база задач по математике.

Оглавление