Фаддеев Д.К.

Лекции по алгебре

Москва
«Книга по Требованию»

УДК 51
ББК 22.1
Ф15

Фаддеев Д.К.
Ф15 Лекции по алгебре / Фаддеев Д.К. – М.: Книга по Требованию, 2013. – 416 с.

ISBN 978-5-458-25543-1

Книга представляет собой изложение курса лекций по алгебре, читавшегося автором в Ленинградском университете на протяжении ряда лет. Этот курс рассчитан на 3 семестра. Большим достоинством книги является то, что абстрактные понятия вводятся в ней как результаты обобщения конкретного математического материала.Для студентов университетов и пединститутов.

ISBN 978-5-458-25543-1

© Издание на русском языке, оформление
«YOYO Media», 2013
© Издание на русском языке, оцифровка,
«Книга по Требованию», 2013

Эта книга является репринтом оригинала, который мы создали специально для Вас, используя запатентованные технологии производства репринтных книг и печати по требованию.

Сначала мы отсканировали каждую страницу оригинала этой редкой книги на профессиональном оборудовании. Затем с помощью специально разработанных программ мы произвели очистку изображения от пятен, клякс, перегибов и попытались отбелить и выровнять каждую страницу книги. К сожалению, некоторые страницы нельзя вернуть в изначальное состояние, и если их было трудно читать в оригинале, то даже при цифровой реставрации их невозможно улучшить.

Разумеется, автоматизированная программная обработка репринтных книг – не самое лучшее решение для восстановления текста в его первозданном виде, однако, наша цель – вернуть читателю точную копию книги, которой может быть несколько веков.

Поэтому мы предупреждаем о возможных погрешностях восстановленного репринтного издания. В издании могут отсутствовать одна или несколько страниц текста, могут встретиться невыводимые пятна и кляксы, надписи на полях или подчеркивания в тексте, нечитаемые фрагменты текста или загибы страниц. Покупать или не покупать подобные издания – решать Вам, мы же делаем все возможное, чтобы редкие и ценные книги, еще недавно утраченные и несправедливо забытые, вновь стали доступными для всех читателей.

Серия Книжный Ренессанс
www.samizday.ru/reprint

Глава XIII

ЕВКЛИДОВО И УНИТАРНОЕ ПРОСТРАНСТВА

Глава XIV

ЭЛЕМЕНТЫ АЛГЕБРЫ ТЕНЗОРОВ

Глава XV

АЛГЕБРЫ

ПРЕДИСЛОВИЕ

Настоящая книга представляет собой обработку лекций по алгебре, читавшихся мной на математико-механическом факультете Ленинградского государственного университета на протяжении нескольких десятилетий для математиков всех специальностей.

От года к году содержание лекций несколько менялось. Здесь собрано теоретико-множественное объединение материала, читавшегося в разные годы.

В основу книги положены лекции, которые я читал в последний раз в 1977—1978 гг. Лекции были старательно записаны Л. Ю. Колотилиной, за что я приношу ей глубокую благодарность.

В ЛГУ линейная алгебра не отделена от общего курса алгебры и читается на третьем семестре. В соответствии с этим последние главы, начиная с главы XII, посвящены линейной алгебре. Элементарно-калькулятивная часть линейной алгебры, состоящая из теории матриц, определителей и квадратичных форм, занимает главы IV и V; этот материал излагается в ЛГУ на первом семестре.

Язык книги несколько архаичен из-за того, что я не тороплюсь вводить абстрактные понятия во избежание формализма при их восприятии. Я считаю, что их следует вводить по мере того, как удается возбудить в учащихся потребность в обобщении или, по крайней мере, если имеется возможность достаточно иллюстрировать общие понятия более конкретным материалом.

Оформление рукописи было бы для меня невозможным, если бы не энергичная помощь моих товарищей по работе в ЛОМИ. Всем им моя глубокая благодарность!

Д. К. Фаддеев

ГЛАВА I

ЦЕЛЫЕ ЧИСЛА

Изучение свойств целых чисел составляет содержание раздела математики, имеющего название «арифметика» или «теория чисел». Обычно первый термин относится к кругу самых элементарных вопросов, в основном, к правилам вычислений с целыми числами, а второй — к установлению более глубоких и нетривиальных свойств целых чисел. Цель этого раздела курса — познакомить читателя с самыми простыми идеями и фактами теории чисел.

§ 1. Теория делимости целых чисел

1. Определение делимости и простейшие свойства этого отношения. Множество всех целых чисел принято обозначать $\mathbb{Z}$. Множество $\mathbb{Z}$ состоит из натуральных, т. е. целых положительных чисел 1, 2, 3, ..., числа 0 и целых отрицательных чисел -1, -2, -3, ... Ясно, что сумма, разность и произведение двух целых чисел суть снова целые числа. Частное же от деления двух целых чисел может и не быть целым числом. Говорят, что целое число a *делится* на целое число b, если существует такое целое число c, что $a = bc$. Другими словами, a делится на b, если их частное c снова есть целое число. То же отношение делимости a на b может быть выражено другими равнозначными терминами: b *делит* a; b — *делитель* a; a есть *кратное* для b. Из определения делимости ясно, что число 0 делится на любое целое число, в том числе и на 0, но ни одно целое число, отличное от нуля, на нуль не делится. Ясно также, что любое целое число a делится на a, $-a$, 1 и -1. Эти числа называются *несобственными*, или *тривиальными*, делителями числа a. Остальные же делители, если они есть, называются *собственными*, или *нетривиальными*.

Запишем теперь в виде предложений (слово «предложение» значит то же, что слово «теорема», — это высказывание, которое должно быть доказано; мы будем пользоваться словом «теорема» только тогда, когда нужно подчеркнуть важность содержания) некоторые простейшие свойства делимости.

Предложение 1. *Если два целых числа a и b делятся на целое число c, то их сумма и разность тоже делятся на c.*

Доказательство. Имеем $a = cg$, $b = ch$, где g и h — целые числа, ибо a и b делятся на c. Тогда $a \pm b = cg \pm ch = c(g \pm h)$. Числа $g \pm h$ целые. Следовательно, числа $a \pm b$ делятся на c.

Предложение 2. *Если целое число a делится на целое число b и k — целое число, то ak делится на b.*

Доказательство. Имеем $a = bm$ при целом m, ибо a делится на b. Тогда $ak = bmk$. Число mk целое. Следовательно, ak делится на b, что и требовалось доказать.

Это предложение можно сформулировать и так: если c делится на a и a делится на b, то c делится на b. Действительно, «c делится на a» значит то же самое, что $c = ak$ при целом k.

2. Деление с остатком. Всем хорошо известно, что если деление целых чисел не выполняется «нацело», то возможно деление «с остатком». Придадим этому высказыванию точный смысл в виде следующей теоремы.

Теорема 3. *Пусть $a, b \in \mathbb{Z}$ (т. е. a и b являются целыми числами) и $b \neq 0$. Существуют целые числа q (неполное частное) и r (остаток) такие, что $a = bq + r$ и $0 \leqslant r \leqslant |b| - 1$. Эти требования однозначно определяют q и r.*

Доказательство. Положим сначала, что $b > 0$. Рассмотрим рациональное (не обязательно целое) число $\alpha = \frac{a}{b}$. Если оно целое, то положим $q = \alpha$. Если же α не целое, то найдутся два соседних целых числа, в промежуток между которыми попадает α. Меньшее из них обозначим через q. Тогда $q < \alpha < q + 1$. Итак, в обоих случаях мы нашли целое число q такое, что $q \leqslant \frac{a}{b} < q + 1$. Умножим все три части этого двойного неравенства на b. Так как $b > 0$, знаки неравенства должно сохранить:

$$bq \leqslant a < bq + b,$$

откуда $0 \leqslant a - bq < b$. Положим $a - bq = r$. Это целое число, и, так как $r < b$, а числа r и b оба целые, должно выполняться более сильное неравенство $r \leqslant b - 1$. Итак, $a = bq + r$ и $0 \leqslant r \leqslant b - 1$.

Пусть теперь $b < 0$. Тогда $b = -|b|$. Применив предыдущее построение к числам a и $|b|$, найдем целые числа q' и r такие, что $a = q'|b| + r$, $0 \leqslant r \leqslant |b| - 1$. Полагая $q' = -q$, получим $a = q(-|b|) + r = qb + r$, $0 \leqslant r \leqslant |b| - 1$. Тем самым существование q и r доказано как для положительных, так и для отрицательных b.

Остается доказать единственность чисел q и r. Пусть $a = bq_1 + r_1$, $0 \leqslant r_1 \leqslant |b| - 1$, и $a = bq_2 + r_2$, $0 \leqslant r_2 \leqslant |b| - 1$, причем, разумеется, числа a, b, q_1, q_2, r_1, r_2 — все целые. Тогда $bq_1 + r_1 = bq_2 + r_2$, $b(q_1 - q_2) = r_2 - r_1$. Положим, что $q_1 \neq q_2$. Тогда $|r_2 - r_1| = |b| \cdot |q_1 - q_2| \geqslant |b|$, ибо $|q_1 - q_2| \geqslant 1$. С другой стороны, самое большее возможное значение для $r_2 - r_1$ есть $|b| - 1 - 0 = |b| - 1$, самое меньшее: $0 - (|b| - 1) = -(|b| - 1)$. Таким образом, $-(|b| - 1) \leqslant r_2 - r_1 \leqslant |b| - 1$, откуда $|r_2 - r_1| \leqslant |b| - 1$, что противоречит установленному ранее $|r_2 - r_1| \geqslant |b|$. Мы пришли к противоречию, доказывающему неверность сделан-

ного предположения $q_1 \neq q_2$. Следовательно, $q_1 = q_2$, а тогда и $r_1 = r_2$. Теорема доказана.

Замечание. По ходу доказательства мы использовали то обстоятельство, что для любого вещественного α (у нас α было рациональным) найдется целое q такое, что $q \leqslant \alpha < q + 1$. Такое число q называется *целой частью* α и обозначается $[\alpha]$. Например, $[5] = 5$, $[\pi] = 3$, $[-2, 7] = -3$.

3. Наибольший общий делитель. Пусть a и b — два целых числа, из которых по крайней мере одно отлично от нуля. *Наибольшим общим делителем* чисел a и b называется наибольшее натуральное число d, являющееся делителем как для a, так и для b.

Например, наибольший общий делитель чисел —6 и 10 равен 2, наибольший общий делитель чисел —6 и 0 есть 6, наибольший общий делитель чисел —6 и 5 равен 1.

Наибольший общий делитель чисел a и b обозначается н. о. д.(a, b) или просто (a, b); последнее обозначение применяется только в случае, если в том же контексте символ (a, b) не используется в каком-либо другом смысле (например, координаты точки на плоскости или скалярное произведение векторов a и b и т. д.).

Важное свойство наибольшего общего делителя сформулировано в следующей теореме.

Теорема 4. *Пусть a, b — целые числа, одно из которых отлично от 0, и пусть d — их наибольший общий делитель. Тогда*

(1) *существуют целые числа u_0, v_0 такие, что $d = au_0 + bv_0$;*

(2) *если d' — какой-либо общий делитель чисел a и b, то d делится на d'.*

Доказательство. Рассмотрим бесконечное множество M целых чисел, состоящее из чисел $au + bv$, где u и v независимо друг от друга пробегают все целые числа: $M = \{au + bv \mid u, v \in Z\}$.

Множество M содержит число a, оно получается при $u = 1$, $v = 0$; M содержит b (при $u = 0$, $v = 1$); M содержит 0 (при $u = 0$, $v = 0$) и бесконечно много других целых чисел.

Установим, что если два числа x и y принадлежат M и $y \neq 0$, то остаток при делении x на y тоже принадежит M. Действительно, $x \in M$ и $y \in M$ значит, что $x = au_1 + bv_1$, $y = au_2 + bv_2$ при некоторых целых u_1, v_1, u_2, v_2. Пусть $x = yq + r$, $q, r \in Z$ и $0 \leqslant r \leqslant |y| - 1$, так что r есть остаток при делении x на y. Тогда $r = x - yq = au_1 + bv_1 - q(au_2 + bv_2) = a(u_1 - qu_2) + b(v_1 - qv_2)$. Числа $u_1 - qu_2$ и $v_1 - qv_2$ целые, следовательно, $r \in M$.

Выберем теперь в множестве M наименьшее положительное число d. Покажем, что a и b делятся на d. Пусть r_1 — остаток при делении a на d. Так как a и d принадлежат M, то, в силу только что сказанного, r_1 принадлежит M. Но $0 \leqslant r_1 < d$, а d — наименьшее положительное число, содержащееся в M. Следова-

тельно, r_1 не может быть положительным числом, так что $r_1 = 0$. Это значит, что a делится на d. Те же соображения приводят к выводу, что b делится на d. Таким образом, d есть общий делитель a и b. Далее, так как $d \in M$, существуют целые u_0 и v_0 такие, что $d = au_0 + bv_0$. Пусть теперь d' — какой-либо общий делитель для a и b. Из равенства $d = au_0 + bv_0$ заключаем, что d делится на d', ибо оба слагаемых правой части равенства делятся на d'. Поэтому $d \geqslant d'$, так что d есть наибольший общий делитель. По ходу рассуждения оказались доказанными оба утверждения теоремы.

4. Алгорифм Евклида. Метод доказательства теоремы 2 очень быстро приводит к цели, но он не дает средства для фактического вычисления d. Предлагаемый способ — найти наименьшее натуральное число в бесконечном множестве чисел M — совершенно не эффективен. Однако деление с остатком позволяет быстро «спускаться» внутри M к наименьшему натуральному числу, содержащемуся в M, т. е. к наибольшему общему делителю. Именно, поделим с остатком a на b (считаем, что $b \neq 0$), затем b на первый остаток, затем первый на второй и т. д. Получим цепочку равенств и неравенств:

$$a = bq_1 + r_1,\ 0 < r_1 \leqslant |b| - 1,\ b = r_1q_2 + r_2,\ 0 < r_2 \leqslant r_1 - 1 \text{ и т. д.}$$

Каждый последующий остаток есть натуральное число, строго меньшее предыдущего. Поэтому процесс не может продолжаться без конца. Но закончиться он может только на том, что на каком-то шагу деление выполнится без остатка. Таким образом,

$$\begin{aligned}
a &= bq_1 + r_1, && 0 < r_1 \leqslant |b| - 1;\\
b &= r_1q_2 + r_2, && 0 < r_2 \leqslant r_1 - 1;\\
r_1 &= r_2q_3 + r_3, && 0 < r_3 \leqslant r_2 - 1;\\
&\ldots\ldots && \ldots\ldots\\
r_{k-2} &= r_{k-1}q_k + r_k, && 0 < r_k \leqslant r_{k-1} - 1;\\
r_{k-1} &= r_kq_{k+1}.
\end{aligned}$$

Покажем, что последний отличный от нуля остаток r_k равен н. о. д. (a, b). Для этого сначала пересмотрим все равенства снизу вверх: r_{k-1} делится на r_k, r_{k-2}, как сумма двух чисел, делящихся на r_k, тоже делится на r_k и т. д. К третьему сверху равенству мы придем, зная, что r_2 и r_3 делятся на r_k, и заключим отсюда, что r_1 делится на r_k. Из второго заключим, что b делится на r_k, из первого — что a делится на r_k. Таким образом, a и b делятся на r_k.

Пусть теперь d' — какой-либо общий делитель для a и b. Пересмотрим равенства сверху вниз с точки зрения делимости на d'. Из первого равенства заключаем, что r_1 как разность двух чисел, делящихся на d', делится на d'. Из второго — что r_2 делится на d' по той же причине, и т. д. Из предпоследнего заключим, что

r_k делится на d' и, следовательно, $r_k \geqslant d'$. Итак, r_k оказывается общим делителем, причем наибольшим.

Изложенный способ отыскания н. о. д. называется *алгорифмом Евклида*, он известен уже более 2000 лет. В процессе доказательства мы вновь установили свойство (2) н. о. д. Далее, из сказанного ранее ясно, что все остатки $r_1, r_2, \ldots, r_k$ принадлежат множеству M, что дает доказательство и свойства (1), причем представление остатков в виде $au + bv$ легко осуществляется шаг за шагом. Таким образом, алгорифм Евклида дает не только способ вычисления н. о. д. чисел a и b, но и его линейное представление в виде $au_0 + bv_0$.

Пример. Пусть $a = 959$, $b = 343$. Найти их н. о. д. и найти его линейное представление.

Решение: $959 = 343 \cdot 2 + 273$; $343 = 273 \cdot 1 + 70$; $273 = 70 \cdot 3 + 63$; $70 = 63 \cdot 1 + 7$; $63 = 7 \cdot 9 + 0$. Таким образом, $d = 7$.

Далее, $273 = 959 - 343 \cdot 2$; $70 = 343 - 273 \cdot 1 = 343 - (959 - 343 \cdot 2) \cdot 1 = 343 \cdot 3 - 959$; $63 = 273 - 70 \cdot 3 = 959 - 343 \cdot 2 - (343 \cdot 3 - 959) \cdot 3 = 959 \cdot 4 - 343 \cdot 11$; $7 = 70 - 63 = 343 \cdot 3 - 959 - (959 \cdot 4 - 343 \cdot 11) = 343 \cdot 14 - 959 \cdot 5$. Таким образом, $7 = 959 \cdot u_0 + 343 \cdot v_0$ при $u_0 = -5$; $v_0 = 14$.

5. **Взаимно простые числа.** Два целых числа называются *взаимно простыми*, если их н. о. д. равен 1.

Ясно, что если d есть наибольший общий делитель целых чисел a и b, то $\frac{a}{d}$ и $\frac{b}{d}$ суть целые взаимно простые числа. Действительно, то, что эти числа целые, следует из того, что d — общий делитель для a и b. Если δ — наибольший общий делитель $\frac{a}{d}$ и $\frac{b}{d}$, то a и b делятся на $d\delta$, откуда следует, что $\delta = 1$, иначе d не был бы наибольшим общим делителем для a и b.

Предложение 5. *Для того чтобы целые числа a и b были взаимно простыми, необходимо и достаточно существование целых чисел u_0, v_0 таких, что $au_0 + bv_0 = 1$.*

Предложение 5 можно сформулировать и в других терминах: для того чтобы неопределенное уравнение $au + bv = 1$ имело решение u_0, v_0 в целых числах, необходимо и достаточно, чтобы a и b были взаимно просты.

Доказательство. Пусть a и b взаимно просты. Тогда их н. о. д., равный 1, имеет линейное представление: $1 = au_0 + bv_0$. Пусть теперь существуют u_0 и v_0 такие, что $au_0 + bv_0 = 1$. Тогда н. о. д. (a, b) делит au_0 и bv_0, а следовательно, и их сумму, равную 1. Но 1 не имеет натуральных делителей, кроме 1, так что н. о. д. (a, b) равен 1. Предложение доказано полностью.

Предложение 6. *Если целые числа a_1, a_2 взаимно просты с целым числом b, то их произведение a_1a_2 тоже взаимно просто с b.*

Доказательство. Существуют целые u_1, v_1, u_2, v_2 такие, что $a_1u_1 + bv_1 = 1$, $a_2u_2 + bv_2 = 1$ в силу предложения 5. Перемножая эти равенства, получим после очевидных преобразований

$$a_1a_2u_1u_2 + b(a_1u_1v_2 + a_2u_2v_1 + bv_1v_2) = 1,$$

откуда, в силу того же предложения, числа a_1a_2 и b взаимно просты, ибо u_1u_2 и $a_1u_1v_2 + a_2u_2v_1 + bv_1v_2$ — целые числа.

Предложение 7. *Если целые числа a_1, a_2, ..., a_k все взаимно просты с b, то произведение $a_1a_2 \ldots a_k$ тоже взаимно просто с b.*

Доказательство. Применим метод математической индукции. При $k = 2$ предложение верно в силу предложения 6. Допустим, что оно верно для произведения $k - 1$ множителей, и в этом предположении докажем его для k множителей. Запишем $a_1a_2 \ldots a_k$ как $a_1(a_2 \ldots a_k)$. Первый множитель a_1 взаимно прост с b по условию. Второй $a_2 \ldots a_k$ взаимно прост с b в силу индуктивного предположения. Следовательно, мы можем применить предложение 6 и заключить, что $a_1a_2 \ldots a_k$ взаимно просто с b, что и требовалось доказать.

Предложение 8. *Если целые числа a_1, ..., a_k и b_1, ..., b_m таковы, что каждое число a_i, $i = 1, \ldots, k$, взаимно просто с каждым числом b_j, $j = 1, \ldots, m$, то их произведения $a_1 \ldots a_k$ и $b_1 \ldots b_m$ взаимно просты.*

Доказательство. Применив m раз предложение 7 к числам $a_1, \ldots, a_k$ и b_j, $j = 1, \ldots, m$, получим, что числа $b_1, \ldots, b_m$ взаимно просты с числом $a_1 \ldots a_k$. Применяя еще раз предложение 7, получим, что $b_1 \ldots b_m$ взаимно просто с $a_1 \ldots a_k$, что и требовалось доказать.

Предложение 9. *Если целые числа a и b взаимно просты, то при натуральных k и m числа a^k и b^m тоже взаимно просты.*

Для доказательства достаточно в предложении 8 положить $a_1 = \ldots = a_k = a$, $b_1 = \ldots = b_m = b$.

Предложение 10. *Если произведение ab двух целых чисел a и b делится на целое число c и первый множитель a взаимно прост с c, то b делится на c.*

Доказательство. По условию a и c взаимно просты, так что существуют целые u_0 и v_0 такие, что $au_0 + cv_0 = 1$. Умножив это равенство на b, получим $abu_0 + cbv_0 = b$. Первое слагаемое левой части делится на c по условию, второе делится на c тривиальным образом. Следовательно, и их сумма b делится на c, что и требовалось доказать.

Предложение 11. *Если целое число a делится на целые взаимно простые числа b_1 и b_2, то a делится и на их произведение.*

Доказательство. Пусть $a = b_1c$ при целом c. По условию a делится на b_2, а b_1 взаимно просто с b_2. Следовательно, согласно предложению 8 число c делится на b_2, т. е. $c = b_2m$ при целом m. Поэтому $a = (b_1b_2)m$, что и требовалось доказать.

Установленные предложения очень просты и кажутся почти тривиальными. Тем не менее из них можно вывести некоторые не совсем тривиальные следствия.

Выведем, например, что степень с натуральным показателем дробного рационального положительного числа не может быть целым числом.

Действительно, пусть a/b — дробное рациональное число с целым положительным знаменателем b и с целым числителем a. Без нарушения общности можно считать, что числитель и знаменатель взаимно просты, этого можно добиться за счет сокращения на наибольший общий делитель. Пусть это выполнено. Ясно, что $b > 1$, иначе a/b было бы целым. Пусть m — натуральное число. Тогда $(a/b)^m = a^m/b^m$. В силу предложения 7 a^m и b^m взаимно просты. Поэтому a^m не может делиться на b^m, так что a^m/b^m не является целым числом.

Из доказанного следует далее, что если целое положительное число c не является m-й степенью целого числа (при натуральном m), то оно не является m-й степенью дробного рационального числа. Поэтому $\sqrt[m]{c}$ есть либо целое число, либо иррациональное. Так, числа $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, $\sqrt{6}$, $\sqrt{7}$, $\sqrt{8}$, $\sqrt{10}$, ... (пропускаются целые $\sqrt{4}$, $\sqrt{9}$, ...) все иррациональны, также иррациональны и числа $\sqrt[3]{2}$, $\sqrt[3]{3}$, $\sqrt[3]{4}$, $\sqrt[3]{5}$, $\sqrt[3]{6}$, $\sqrt[3]{7}$, $\sqrt[3]{9}$, $\sqrt[3]{10}$, ... (пропускаются целые $\sqrt[3]{8}$, $\sqrt[3]{27}$, ...) и т. д.

6. Простые числа. Целое положительное число, большее единицы, называется *простым*, если оно не имеет целых положительных делителей кроме себя и единицы. Так, числа 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97 простые, а числа 4, 6, 8, 9, 10, 12, 14, ... нет. Непростые числа 4, 6, ... называются также *составными*. Число 1 не относится ни к простым, ни к составным числам.

Предложение 12. *Всякое целое число, большее* 1, *делится по крайней мере на одно простое число.*

Доказательство. Пусть $n > 1$ — целое положительное число. Если оно простое, предложение верно, ибо n всегда делится на себя. Если оно составное, то оно делится на число $n_1 > 1$, меньшее чем n. Если n_1 простое, предложение доказано: n делится на n_1. Если нет, то оно делится на меньшее чем n_1 число n_2 и т. д.

Процесс выделения делителей $n > n_1 > n_2 > \ldots$ оборвется через конечное число шагов, а оборваться он может только на том, что мы придем к простому делителю n_k. Предложение доказано.

Простых чисел существует бесконечно много. Это непосредственно вытекает из следующего предложения.

Предложение 13. *Каково бы ни было конечное множество простых чисел* $\{p_1, p_2, \ldots, p_k\}$, *всегда найдется простое число, не принадлежащее этому множеству.*

Доказательство. Рассмотрим число $n = p_1 p_2 \ldots p_k + 1$. В силу предложения 12 оно делится по крайней мере на одно простое число p. Это число p не может совпадать ни с одним из чисел $p_1, p_2, \ldots, p_k$. Действительно, если $p = p_i$, то 1 делится на p_i как разность двух чисел, делящихся на p_i, что невозможно.

Это рассуждение было известно еще Евклиду.

Предложение 14. *Если целое число n не делится на простое число p, то n и p взаимно просты.*

Доказательство. Пусть $d = (n, p)$. Так как p делится на d и p простое, для d имеются только две возможности: $d = p$ или $d = 1$. В первом случае n делится на p, во втором n и p взаимно просты, что и требовалось доказать.

Из предложения 14 вытекает следующее утверждение.

Предложение 15. *Если p_1 и p_2 — два различных простых числа, то они взаимно просты.*

Действительно, меньшее из них не делится на большее, и, следовательно, они взаимно просты.

Предложение 16. *Если произведение двух целых чисел делится на простое число, то по крайней мере один из сомножителей делится на это простое число.*

Действительно, пусть ab делится на p, где $a, b \in \mathbb{Z}$, p — простое. Если a делится на p, то предложение справедливо. Если a не делится на p, то a и p взаимно просты, а тогда, согласно предложению 10, b делится на p.

Это предложение легко обобщается.

Предложение 17. *Если произведение нескольких целых чисел делится на простое число, то на него делится хотя бы один из сомножителей.*

Доказательство. Применим метод математической индукции по числу сомножителей. База есть — предложение верно для двух сомножителей. Допустим, что оно верно для произведения $k - 1$ сомножителей. Пусть теперь $a_1 a_2 \ldots a_k$ делится на простое число p. Так как $a_1 a_2 \ldots a_k = a_1 (a_2 \ldots a_k)$, заключаем на основании предложения 14, что либо a_1 делится на p, либо произведение $a_2 \ldots a_k$ делится на p. Во втором случае, в силу индуктивного предположения, один из сомножителей $a_2, \ldots, a_k$ делится на p, а в первом a_1 делится на p. Тем самым предложение доказано.

Теперь мы в состоянии доказать основную теорему теории делимости целых чисел.

Теорема 18. *Каждое натуральное число, большее единицы, может быть представлено в виде произведения простых сомножителей, и два таких разложения могут отличаться только порядком следования сомножителей.*

Доказательство. Применим метод индукции. Для числа 2 утверждение теоремы тривиально (так же, как и для всякого простого числа). Допустим, что теорема верна для всех натуральных