

И.К. Кикоин

Журнал Квант 1978 №10

Москва
«Книга по Требованию»

УДК 50
ББК 22
К38

К38 **Кикоин И.К.**
Журнал Квант 1978 №10 / И.К. Кикоин – М.: Книга по Требованию, 2023. – 100 с.

ISBN 978-5-458-30647-8

Журнал Квант 1978 №10

ISBN 978-5-458-30647-8

© Издание на русском языке, оформление
«YOYO Media», 2023
© Издание на русском языке, оцифровка,
«Книга по Требованию», 2023

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 первоизданном 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.

Л. Н. Толстого на преподавание арифметики. Многие идеи Л. Н. Толстого явно перекликаются с современными взглядами на преподавание математики в школе. Вот только один пример: «Уравнение, — писал Л. Н. Толстой, — следовательно, алгебру я начинаю вместе с первыми действиями...» (Л. Н. Толстой. Педагогические сочинения. М., 1953). Кажется, что это сказано не сто лет назад, а сегодня, о новых учебниках для начальных классов.

Л. Н. Толстой всю жизнь любил интересные, оригинальные задачи, высоко ценил простые и прозрачные решения. Напомним читателям одну из его любимых задач — «задачу о косцах», — которая решается нехитрыми рассуждениями без составления уравнений.

«Артели косцов надо было скосить два луга, один вдвое больше другого. Половину дня артель косила большой луг. После этого артель разделилась пополам: первая половина осталась на большом лугу и докосила его к вечеру до конца; вторая же половина косила малый луг, на котором к вечеру еще остался участок, скошенный на другой день одним косцом за один день работы. Сколько косцов было в артели?»

В «Войне и мире» многие страницы посвящены раздумьям писателя о жизни, о Родине, о бытии, о человеке. И чем больше перечитываешь это произведение, тем больше находишь в нем нового, глубокого, неожиданного, ранее скрытого.

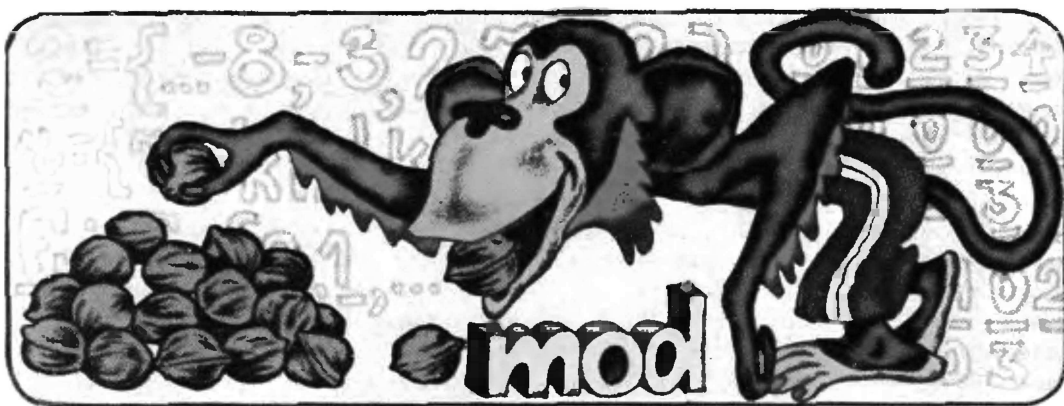
Ниже мы воспроизводим отрывок из романа, где речь идет об одном из важнейших вопросов философии естествознания, тесно примыкающем к тематике нашего журнала.

Для человеческого ума непонятна абсолютная непрерывность движения. Человеку становятся понятны законы какого бы то ни было движения только тогда, когда он рассматривает произвольно взятые единицы этого движения. Но вместе с тем из этого-то произвольного деления непрерывного движения на прерывные единицы происходит большая часть человеческих заблуждений.

Известен так называемый софизм древних, состоящий в том, что Ахиллес никогда не догонит впереди идущую черепаху, несмотря на то, что Ахиллес идет в десять раз скорее черепахи: как только Ахиллес пройдет пространство, отделяющее его от черепахи, черепаха пройдет впереди его одну десятую этого пространства; Ахиллес пройдет эту десятую, черепаха пройдет одну сотую и т. д. до бесконечности. Задача эта представлялась древним неразрешимой. Бессмысленность решения (что Ахиллес никогда не догонит черепаху) вытекала из того только, что произвольно были допущены прерывные единицы движения, тогда как движение и Ахиллеса и черепахи совершалось непрерывно.

Принимая все более и более мелкие единицы движения, мы только приближаемся к решению вопроса, но никогда не достигаем его. Только допустив бесконечно-малую величину и восходящую от нее прогрессию до одной десятой и взяв сумму этой геометрической прогрессии, мы достигаем решения вопроса. Новая отрасль математики, достигнув искусства обращаться с бесконечно-малыми величинами, и в других более сложных вопросах движения дает теперь ответы на вопросы, казавшиеся неразрешимыми.

Эта новая, неизвестная древним, отрасль математики, при рассмотрении вопросов движения, допуская бесконечно-малые величины, то есть такие, при которых восстанавливается главное условие движений (абсолютная непрерывность), тем самым исправляет ту неизбежную ошибку, которую ум человеческий не может не делать, рассматривая вместо непрерывного движения отдельные единицы движения.



Н. Виленкин

Сравнения и классы вычетов

Многим любителям математики известна следующая задача:

Обезьяна и орехи

Пять путешественников остановились на ночлег. Они везли с собой мешок орехов и обезьяну. Ночью один из них проснулся, подошел к мешку и разделил орехи на 5 равных частей, причем один орех остался лишним. Он отдал обезьяне лишний орех, съел свою долю и снова лег спать. Потом проснулся второй путешественник и, не зная о поступке первого, проделал то же самое. Потом это же сделали по очереди остальные три путешественника. Когда утром оставшиеся орехи разделили на 5 равных частей, снова остался один орех для обезьяны. Сколько было орехов?

Вся трудность этой задачи в лиших орехах, без них ответом послужило бы любое число, которое можно шесть раз делить без остатка на 5, то есть любое число, кратное $5^6 = 15625$. А из-за того, что каждый раз деление происходило с остатком, задачу решить куда труднее. Замечательное решение придумал в сту-

денческие годы знаменитый английский физик Дирак. Он решил найти число орехов, которое бы ... не менялось при описанной операции (делении на пять частей с выделением ореха обезьяне и поедании одной части). Читатель, несомненно, скажет, что такого числа орехов быть не может — ясно, что после этой операции оно должно уменьшиться. Но все дело в том, что Дирак не ограничивал себя натуральными числами. А тогда ему осталось решить уравнение $\frac{4}{5}(x-1) = x$. Корнем этого уравнения является число -4 . Поэтому число -4 могло бы быть решением нашей задачи, но по ее смыслу, конечно, не годится. Зато теперь ясно, как получить положительный ответ: надо к числу -4 , найденному Дираком, прибавить 5^6 . Проверьте, что ответ 15621 удовлетворяет условию задачи. Впрочем, ему удовлетворяет и каждое число вида $-4 + 5^6 \cdot k$, где k — любое натуральное число.

Что такое сравнимые числа

Если отвлечься от требования положительности решения, то любое число вида $-4 + 5^6 \cdot k$, где k — целое, является решением задачи про орехи и обезьяну. Эти числа образуют «двустороннюю арифметическую прогрессию» с разностью 5^6 , простирающуюся в обе стороны. У них есть одно общее свойство — при делении на 5^6 все они дают один и тот же остаток 15621 .

Про такие числа в математике говорят, что они *сравнимы друг с другом по модулю**) 15 625.

В общем виде понятие сравнимости по некоторому модулю $m \in \mathbb{N}$ можно определить двумя равносильными способами:

Определение 1. Целые числа a и b называются *сравнимыми по модулю m* , если их разность делится без остатка на m .

Определение 1'. Целые числа a и b называются *сравнимыми по модулю m* , если их остатки при делении на m одинаковы**).

Если числа a и b сравнимы друг с другом по модулю m , то пишут так:

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

Например, $16 \equiv 30 \pmod{7}$, так как разность $16 - 30 = -14$ делится на 7, а $72 \not\equiv 45 \pmod{8}$, так как $72 - 45 = 27$ не делится на 8.

Арифметика остатков

Все числа, сравнимые с числом 2 по модулю 5, одинаково ведут себя при делении на 5 — они дают остаток 2. Объединим эти числа в одно множество и назовем его *классом вычетов по модулю 5*. Обозначим этот класс той же цифрой 2, только, чтобы отличить его от числа 2, будем писать ее так: $\bar{2}$. Значит, $\bar{2}$ — не число, а бесконечная совокупность чисел:

$$\bar{2} = \{\dots -8, -3, 2, 7, 12, \dots\}$$

Так же определяется класс вычетов по любому модулю m . При делении на m могут получиться m различных остатков: 0, 1, 2, ..., $m-1$. Каждому из них соответствует свой класс вычетов. Остатку r соответствует класс вычетов $\bar{r}$, состоящий из чисел вида $r + km$, где k — целое число:

$$\bar{r} = \{r + km \mid k \in \mathbb{Z}\}.$$

Все множество $\mathbb{Z}$ целых чисел распадается на m классов вычетов по

модулю m . Множество всех этих классов обозначают через F_m : $F_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$. При изучении вопросов, касающихся делимости на m , лучше иметь дело с конечным множеством F_m , чем с бесконечным множеством $\mathbb{Z}$.

Чтобы решать задачи про делимость, надо уметь выполнять над классами вычетов арифметические операции. Начнем со сложения. Оно определяется очень просто — в каждом из слагаемых (напомним, что класс вычетов есть бесконечное множество целых чисел) берут по представителю и складывают их, а потом смотрят, в какой класс вычетов попала сумма. Его и называют *суммой данных классов*. Например, сложим классы вычетов $\bar{4}$ и $\bar{5}$ по модулю 6. Для этого выберем в них по представителю. Чтобы долго не думать, возьмем сами остатки $\bar{4}$ и $\bar{5}$, давшие названия слагаемым классам. Их сумма равна 9. Но $9 \equiv 3 \pmod{6}$ и потому $\bar{4} + \bar{5} = \bar{3}$. Если те же классы берутся не в F_6 , а в F_8 , то сумма получится иная: $\bar{4} + \bar{5} = \bar{1}$. А в F_9 $\bar{4} + \bar{5} = \bar{0}$.

Чтобы покончить с вопросом о сложении классов вычетов, надо еще доказать, что при выборе иных представителей сумма не изменится. Это следует из такой теоремы:

Теорема 1. Если $a \equiv a_1 \pmod{m}$ и $b \equiv b_1 \pmod{m}$, то $a + b \equiv a_1 + b_1 \pmod{m}$.

Доказательство. Так как $a \equiv a_1 \pmod{m}$, $a = a_1 + km$, где $k \in \mathbb{Z}$, а так как $b \equiv b_1 \pmod{m}$, $b = b_1 + lm$, где $l \in \mathbb{Z}$. Поэтому $a + b = a_1 + b_1 + (k + l)m$, где $k + l \in \mathbb{Z}$, и $a + b \equiv a_1 + b_1 \pmod{m}$.

Мы свели сложение классов вычетов к сложению чисел. Поэтому сложение классов вычетов коммутативно и ассоциативно, то есть $\bar{a} + \bar{b} = \bar{b} + \bar{a}$ и $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$, прибавление класса $\bar{0}$ не меняет класса вычетов, то есть $\bar{a} + \bar{0} = \bar{a}$, и т. д.

Вычитание и умножение классов вычетов определяются точно так же — в классе выбирают по представителю и выполняют операции над ними. И здесь результат не зависит от выбо-

*) Слово «модуль» происходит от латинского *modulus* (мера).

**) *Остатком* от деления целого числа a на натуральное число m называется такое число r , что $a = mq + r$ и $0 \leq r < m$.

ра представителей (докажите это сами). Более того, справедливо следующее весьма общее утверждение:

Если $P(x)$ — многочлен с целыми коэффициентами и $a \equiv a_1 \pmod{m}$, то $P(a) \equiv P(a_1) \pmod{m}$. Постарайтесь доказать это самостоятельно.

Свойства операций вычитания и умножения классов вычетов тоже очень похожи на свойства этих операций для целых чисел (за одним исключением; о нем — ниже).

Задачи на делимость

Поскольку классы вычетов по модулю m тесно связаны с остатками от деления на m , почти все задачи, в которых речь идет о делимости чисел, удобно решать с помощью сравнений.

Пример 1. Найдём остаток от деления 212^{1978} на 7.

Так как при делении 212 на 7 получается остаток 2, $212 \equiv 2 \pmod{7}$. Отсюда следует, что $212^{1978} \equiv 2^{1978} \pmod{7}$. Заметим теперь, что $2^3 = 8 \equiv 1 \pmod{7}$. Но $1978 = 659 \times 3 + 1$. Значит, из $2^3 \equiv 1 \pmod{7}$ следует, что $2^{1978} = (2^3)^{659} \cdot 2 \equiv 1^{659} \cdot 2 \equiv 2 \pmod{7}$. Поэтому при делении 212^{1978} на 7 получится остаток 2.

Пример 2. Выведем признак делимости на 9.

Так как $10 \equiv 1 \pmod{9}$, для любого k имеем $10^k \equiv 1 \pmod{9}$. Но тогда

$$a_0 \cdot 10^n + a_1 \cdot 10^{n-1} + \dots + a_n \equiv a_0 + a_1 + \dots + a_n \pmod{9}.$$

Это значит, что числа $N = a_0 \cdot 10^n + \dots + a_n$ и $M = a_0 + \dots + a_n$ имеют одинаковые остатки при делении на 9. В частности, N делится на 9 в том и только в том случае, когда на 9 делится число M (сумма цифр числа N).

Пример 3. Докажем, что квадрат любого натурального числа либо делится на 9, либо даёт при делении на 3 остаток 1.

В самом деле, если $x \equiv 0 \pmod{3}$, то x^2 делится на 9. Если же $x \equiv 1 \pmod{3}$ или $x \equiv 2 \pmod{3}$, то $x^2 \equiv 1 \pmod{3}$, так как $1^2 \equiv 1$ и $2^2 \equiv 4 \equiv 1 \pmod{3}$.

Пример 4. Найдём последнюю цифру числа 7^{7^7} .

Нам надо найти остаток от деления числа 7^{7^7} на 10. Но $7^2 = 49 \equiv -1 \pmod{10}$, и потому $7^4 \equiv (-1)^2 \equiv 1 \pmod{10}$. Найдём остаток от деления показателя 7^7 на 4. Так как $7 \equiv -1 \pmod{4}$, $7^2 \equiv (-1)^2 \equiv 1 \pmod{4}$, и потому $7^7 \equiv 1m + 3$. Следовательно, $7^{7^7} = (7^4)^m \cdot 7^3 \equiv (-1)^3 \equiv -1 \equiv 9 \pmod{10}$. Это значит, что у чисел 7^{7^7} и 3 одинакова последняя цифра, то есть 7^{7^7} кончается на 3.

Деление классов вычетов

Разделить класс вычетов $\bar{b}$ на класс вычетов $\bar{a}$ — значит найти такой класс вычетов $\bar{x}$, что $\bar{a}\bar{x} = \bar{b}$. Для целых чисел задача деления разрешима не всегда, но уж если она решается, то единственным образом. Это связано с тем, что произведение двух целых чисел равно нулю лишь в случае, когда хотя один из множителей равен нулю. Но в F_m дело обстоит не так. Взглянув на таблицу умножения для F_6 , замечаем, что нули стоят в ней не только в первой строке и первом столбце (там, где один из множителей равен нулю).

Нулю равны и произведения $\bar{2} \cdot \bar{3}$, $\bar{3} \cdot \bar{4}$, хотя множители отличны от нуля. Как говорят, в F_6 есть делители нуля (класс вычетов $\bar{a}$ называется делителем нуля, если он отличен от $\bar{0}$, но существует такой класс $\bar{b} \neq \bar{0}$, что $\bar{a} \cdot \bar{b} = \bar{0}$). В F_6 делителями нуля оказались классы $\bar{2}$, $\bar{3}$, $\bar{4}$. Числа 2, 3, 4 имеют общее свойство — они не являются взаимно простыми с модулем 6. Это наводит на мысль о справедливости следующей теоремы:

Таблица умножения в F_6

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Теорема 2. Класс вычетов $\bar{a}$ в F_m не является делителем нуля в том и только в том случае, когда a и m взаимно просты.

Доказательство. Пусть a и m взаимно просты. Если $\bar{a} \cdot \bar{b} = \bar{0}$, то число ab делится на m . Но, в силу взаимной простоты a и m , это может быть лишь в случае, когда b делится на m , то есть $\bar{b} = \bar{0}$. Это и значит, что $\bar{ab} = \bar{0}$ лишь при $\bar{b} = \bar{0}$, то есть что $\bar{a}$ не является делителем нуля.

Предположим теперь, что наибольший общий делитель чисел a и m отличен от 1, $a = a_1d$, $m = m_1d$, $d > 1$. Тогда число $m_1 < m$ — целое, причем отлично от m , и потому $\overline{m_1} \neq \bar{0}$. Но $am_1 = a_1dm_1 = a_1m$, то есть $am_1 = \bar{0}$. Значит, $\bar{a}$ — делитель нуля.

Если число a взаимно просто с модулем m , то все числа из класса вычетов $\bar{a}$ взаимно просты с m . В этом случае говорят, что класс $\bar{a}$ взаимно прост с m .

Из теоремы 2 вытекает важное **Следствие 1.** Если класс вычетов $\bar{a}$ взаимно прост с m , то в F_m можно однозначно делить на $\bar{a}$, то есть для любого $\bar{b} \in F_m$ уравнение $\bar{a}x = \bar{b}$ имеет одно и только одно решение.

Сначала докажем, что это уравнение не может иметь различных решений. Если $\bar{a}x_1 = \bar{b}$ и $\bar{a}x_2 = \bar{b}$, то $\bar{a}(x_1 - x_2) = \bar{0}$, а так как $\bar{a}$ не делитель нуля, то $\bar{x}_1 - \bar{x}_2 = \bar{0}$, то есть $\bar{x}_1 = \bar{x}_2$. Значит, решение может быть лишь одно.

Осталось показать, что решение существует.

Мы только что доказали, что среди классов вычетов $\bar{a} \cdot \bar{0}$, $\bar{a} \cdot \bar{1}$, ..., $\bar{a} \cdot \overline{(m-1)}$ нет одинаковых. Значит, это те же классы $\bar{0}$, $\bar{1}$, ..., $\overline{m-1}$, только, возможно, взятые в ином порядке. А тогда для любого класса $\bar{b}$ найдется такой класс $\bar{x}$, что $\bar{a} \cdot \bar{x} = \bar{b}$.

Подтверждением доказанного следствия может служить таблица умножения по модулю 6 — из нее видно, что только в строках для классов $\bar{1}$ и $\bar{5}$ встречаются все классы вычетов. В других строках есть лишь

Таблица умножения в F_6

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

часть классов: в строках для $\bar{2}$ и $\bar{4}$ классы $\bar{0}$, $\bar{2}$, $\bar{4}$, а в строке для $\bar{3}$ — классы $\bar{0}$ и $\bar{3}$. Легко понять, как обстоит дело в общем случае:

Следствие 2. Если $(a, m) = d^*$, то уравнение $ax = b$ имеет решение лишь при условии, что b делится на d . В этом случае число решений равно d .

Предоставляем читателю доказать это утверждение.

В случае, когда модуль является простым числом, можно делить на любой ненулевой класс вычетов — в этом случае все такие классы взаимно просты с модулем. Поэтому, например, в таблице умножения по модулю 5 одна строка состоит из нулей, а остальные содержат по одному разу все классы вычетов.

Теоремы Ферма и Эйлера

В теории чисел очень часто применяется так называемая **Малая теорема Ферма**:

Теорема 3. Если p — простое число и a не делится на p , то остаток от деления числа a^{p-1} на p равен 1.

По-другому ее можно сформулировать следующим образом:

Теорема 3'. Если $\bar{a}$ — ненулевой класс вычетов по простому модулю p , то $\bar{a}^{p-1} = \bar{1}$.

Доказательство. Так как $0 < a < p$, а модуль p — простое число, то a и p взаимно просты. Поэтому классы вычетов $\bar{a} \cdot \bar{1}$, $\bar{a} \cdot \bar{2}$, ..., $\bar{a} \cdot \overline{(p-1)}$ являются теми же самыми, что и $\bar{1}, \bar{2}, \dots, \overline{p-1}$, только

*) (a, m) — наибольший общий делитель чисел a и m .

взятыми, быть может, в другом порядке. Так как умножение в F_p коммутативно и ассоциативно, то

$$(\overline{a} \cdot \overline{1}) (\overline{a} \cdot \overline{2}) \dots (\overline{a} \cdot \overline{(p-1)}) = \overline{1} \times \overline{2} \cdot \dots \cdot \overline{(p-1)}.$$

Осталось сократить это равенство на отличный от $\overline{0}$ множитель $\overline{1} \cdot \overline{2} \times \dots \cdot \overline{(p-1)}$, чтобы убедиться в том, что $\overline{a}^{p-1} = \overline{1}$.

В теореме Ферма модуль p обязан быть простым числом. Эйлер открыл замечательное обобщение этой теоремы на случай составного модуля m . Классы вычетов $\overline{1}, \overline{2}, \dots, \overline{p-1}$, которые мы умножали на $\overline{a}$, взаимно просты с p . Возьмем и для составного модуля m лишь классы вычетов, взаимно простые с m , и обозначим их число через $\varphi(m)$. Умножение этих классов на класс вычетов $\overline{a}$, взаимно простой с m , лишь переставляет их. Перемножая эти произведения и рассуждая так же, как при доказательстве Малой теоремы Ферма, приходим к следующему утверждению:

Теорема 4. Если класс вычетов $\overline{a}$ взаимно прост с модулем m , то $\overline{a}^{\varphi(m)} = \overline{1}$ (если число a взаимно просто с m , то при делении $a^{\varphi(m)}$ на m получается остаток 1).

Например, $\varphi(12)=4$: с модулем 12 взаимно просты классы вычетов $\overline{1}, \overline{5}, \overline{7}, \overline{11}$. Число 31 взаимно просто с числом 12. Поэтому при делении 31^4 на 12 получается остаток 1. Проверьте это!

Чтобы успешно применять теорему Эйлера, надо уметь вычислять функцию Эйлера*) $\varphi(m)$. Если m — простое число, то $\varphi(m)=m-1$. Можно доказать что если разложение модуля m на простые множители имеет вид $m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, то

$$\varphi(m) = m \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right).$$

Например, $600 = 2^3 \cdot 3 \cdot 5^2$, и потому

$$\begin{aligned} \varphi(600) &= 600 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \times \\ &\quad \times \left(1 - \frac{1}{5}\right) = 160. \end{aligned}$$

Первообразные корни

Возьмем какой-нибудь класс вычетов $\overline{a}$, взаимно простой с модулем m , и начнем возводить его в квадрат, куб и т. д. Мы уже знаем, что $\overline{a}^{\varphi(m)} = \overline{1}$. Но класс $\overline{1}$ может встретиться и раньше. Например, $\varphi(11)=10$, а в F_{11} уже $\overline{4}^5 = \overline{1}$. В самом деле, $4^5=1024$ и при делении 1024 на 11 получается остаток 1.

Легко доказать, что если k — наименьший положительный показатель, при котором $\overline{a}^k = \overline{1}$, то $\varphi(m)$ делится на k (иначе уже $\overline{a}^r$, где r — остаток от деления $\varphi(m)$ на k , равнялось бы 1).

Назовем класс вычетов $\overline{a}$ (по модулю m), взаимно простой с m , *первообразным корнем*, если для него $\varphi(m)$ — наименьший положительный показатель степени, при котором получается $\overline{1}$. В этом случае все классы вычетов, взаимно простые с m , являются степенями $\overline{a}$. Иными словами, для любого такого класса вычетов $\overline{b}$ найдется показатель k такой, что $\overline{a}^k = \overline{b}$. В этом случае k можно назвать «логарифмом $\overline{b}$ по основанию $\overline{a}$ » — в теории чисел вместо «логарифм» говорят «индекс».

Из сказанного отнюдь не следует, что первообразные корни существуют для всех модулей. Но есть случай, когда ответ заведомо положителен — если модуль является простым числом. Иными словами, если p — простое число, то среди классов вычетов по модулю p найдется хотя бы один первообразный корень. Доказательство этого утверждения вы найдете в следующем номере, в статье «Сравнения по простому модулю».

*) Об этой функции см. «Квант», 1977, № 7, с. 2.



Качества современного автомобиля в значительной степени определяются уровнем развития теории автомобиля. Увеличение скорости автомобиля, его устойчивости, управляемости, плавности хода и улучшение многих других его характеристик требуют непрерывного развития теории, методов расчета и испытаний автомобилей.

Одной из многих интереснейших задач теории автомобиля является задача о критической скорости качения автомобильной шины.

Что такое критическая скорость, от чего зависит значение этой величины, какими способами можно улучшить эту важную характеристику — эти вопросы мы и рассмотрим в настоящей статье.

Начнем с задачи, которая, на первый взгляд, не имеет прямой связи с этими вопросами.

Волна, бегущая по ленте

Рассмотрим «бесконечную» тяжелую ленту, одетую на два вращающихся барабана и «бегущую» со скоростью

V . На участке AB эта лента пропущена через неподвижно закрепленную искривленную трубку (рис. 1). Ось этой трубки представляет собой некоторую плоскую кривую (лежащую в плоскости чертежа). Найти силы, действующие со стороны трубки на ленту. Влиянием силы тяжести пренебречь; считать, что трение между лентой и стенками трубки отсутствует; сила натяжения постоянна (по длине ленты) и равна по модулю $|N|$. Масса единицы длины ленты (погонная масса) равна m .

Рассмотрим малый элемент CD ленты длиной l , который в данный мо-

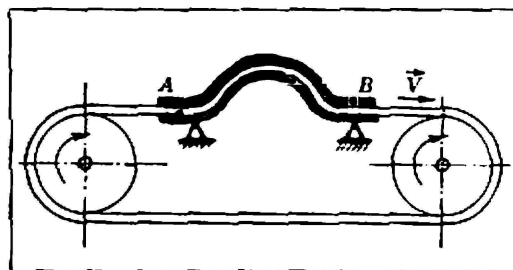


Рис. 1.

мент находится в трубке. Участок трубки, в котором находится этот элемент, можно с хорошим приближением считать дугой окружности. Пусть радиус этой окружности равен R (рис. 2).

Элемент CD движется с постоянной по модулю скоростью V по окружности радиуса R . Следовательно, он имеет центростремительное ускорение, равное V^2/R и направленное к точке O — центру кривизны дуги CD *).

Посмотрим, какие силы сообщают это ускорение элементу CD . Со стороны соседних участков ленты на него действуют силы натяжения N , направленные по касательным к дуге CD в точках C и D (см. рис. 2). Со стороны стенок трубки на ленту действуют силы нормального давления. Пусть на единицу длины ленты действует со стороны трубки сила нормального давления, равная по модулю $|\vec{f}|$. Тогда сила, действующая на

элемент CD , равна $|\vec{f}|l$ (поскольку l мало и $l \ll R$, можно считать, что эта сила равна именно $|\vec{f}|l$, то есть такая же, как если бы элемент CD был прямолинейным). Согласно II закону Ньютона равнодействующая F всех этих сил, направленная к центру кривизны O , и сообщает элементу CD

центростремительное ускорение:

$$ml \frac{V^2}{R} = |\vec{F}| \quad (1)$$

(ml — масса элемента CD). Как видно из рисунка 2, $|\vec{F}| = |\vec{N}'| - |\vec{f}|l$, где N' — равнодействующая сил натяжения, действующих на элемент CD со стороны соседних участков ленты. Учитывая, что угол φ мал и $\sin \varphi \approx \varphi$, находим, что $|\vec{N}'| = 2|\vec{N}|\varphi$, $l = 2R\varphi$. Таким образом, $|\vec{F}| = 2|\vec{N}|\varphi - 2|\vec{f}|R\varphi$.

Подставим это значение $|\vec{F}|$ и $l = 2R\varphi$ в выражение (1):

$$2mR\varphi \frac{V^2}{R} = 2|\vec{N}|\varphi - 2|\vec{f}|R\varphi.$$

Отсюда найдем $|\vec{f}|$:

$$|\vec{f}| = \frac{1}{R} (|\vec{N}| - mV^2). \quad (2)$$

Итак, мы нашли интересовавшую нас силу нормального давления со стороны стенок трубки на ленту. Точнее, мы нашли эту силу, приходящуюся на единицу длины ленты на участке, радиус кривизны которого равен R . Но для дальнейшего рассмотрения нас устроит эта величина.

Проанализируем формулу (2). Величина, стоящая в скобках, не меняется вдоль трубки, так что при данных $|\vec{N}|$, m и $|V|$ значение $|\vec{f}|$ определяется радиусом кривизны трубки: $|\vec{f}|$ пропорционально кри-

* Центр кривизны — центр той окружности, дугой которой является криволинейный участок CD (дуга CD). Величина, обратная радиусу кривизны, называется кривизной.

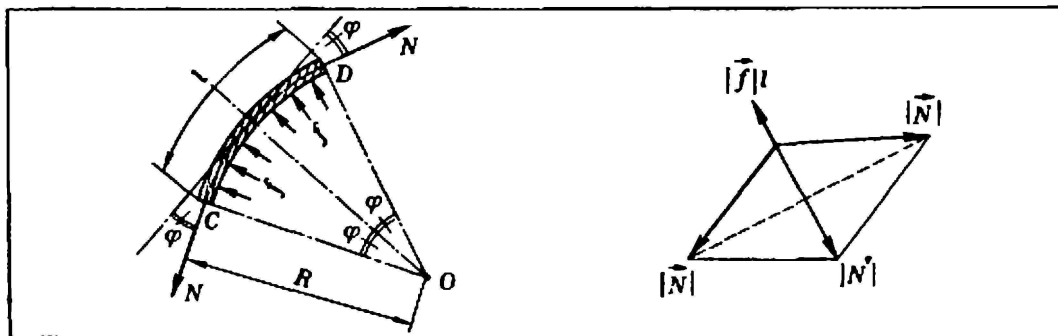


Рис. 2.

визне — $|\vec{f}| \sim \frac{1}{R}$. Если $\vec{V} = 0$ (лента неподвижна), $|\vec{f}| = \frac{|\vec{N}|}{R}$ — сила давления определяется силой натяжения и кривизной трубки в данной точке. С появлением скорости $\vec{V}$ и с ее ростом значение $|\vec{f}|$ начинает уменьшаться и при скорости, равной

$$|\vec{V}| = \sqrt{\frac{|\vec{N}|}{m}}, \quad (3)$$

обращается в нуль сразу по всей длине трубки. Назовем эту скорость критической ($V_{кр}$).

Что это означает — $|\vec{f}| = 0$? Это означает, что при $|\vec{V}| = V_{кр}$ лента не взаимодействует с трубкой. Если именно при таком значении скорости трубку убрать, то искривление, ею вызванное, останется — лента по-прежнему будет изогнута на участке AB .

По отношению к наблюдателю, движущемуся вправо со скоростью, равной по модулю $V_{кр}$, это искривление бежит по ленте влево со скоростью $V_{кр}$. Такое явление называется волной, бегущей по ленте, а скорость $V_{кр}$ — скоростью распространения волны.

Представим себе теперь, что $|\vec{V}| < V_{кр}$ и мы убрали трубку, но сумели приложить к ленте на участке AB силы давления $\vec{f}$, распределенные по длине ленты так же, как от трубки. Ясно, что при этом лента получит точно такое же искривление, какое было при наличии трубки. В каждой точке кривизна ленты $\frac{1}{R}$ будет связана с приложенными силами давления той же формулой (2). Если силы давления $\vec{f}$ поддерживать постоянными, а скорость ленты увеличивать, то, как следует из формулы (2), степень искривленности ленты, характеризуемая величиной $\frac{1}{R}$, будет увеличиваться. (При этом характер распределения величины $\frac{1}{R}$ по длине участка AB будет опреде-

ляться законом распределения сил давления $\vec{f}$ по длине этого участка.)

При неизменном законе распределения сил давления на участке AB и при скорости ленты, близкой к критической, можно, таким образом, получить как угодно большое искривление ленты на участке AB .

Этот вывод можно сформулировать по-другому. Если по ленте «бежит» нагрузка, то есть давления, некоторым образом распределенные на участке AB , и величина этой нагрузки не меняется, а скорость ее распространения относительно ленты растет, то степень искривленности ленты на участке AB возрастает с ростом скорости, а следовательно, возрастет деформация ленты от данной нагрузки. При приближении скорости к $V_{кр}$ искривление ленты будет возрастать неограниченно. С этой точки зрения получается, что при скорости движения нагрузки, близкой к критической, натянутая лента перестает сопротивляться нагрузке.

Полученный вывод не зависит от характера распределения нагрузки на участке AB , так же как выражение для $V_{кр}$ не зависит от формы искривленной трубки.

Перейдем к автомобилю

Понятие критической скорости «бегущей» нагрузки может быть с помощью более сложных рассуждений распространено и на другие случаи, такие, например, как бегущая по рельсу нагрузка от колеса железнодорожного вагона. Рельс также искривляется от этой нагрузки, но задача в этом случае сложнее, так как рельс в отличие от ленты имеет так называемую «жесткость на изгиб» и лежит на «упругом основании» — земле. Однако и в этом случае существует критическая скорость. Расчеты показывают, что эта скорость очень высока (порядка 1000 км/ч) и может иметь практическое значение лишь при создании поездов, движущихся с очень большими, пока неосуществимыми, скоростями.

А вот при движении современного автомобиля существование критической скорости имеет большое прак-

тическое значение. Именно $V_{кр}$ определяет максимальное значение скорости, которую может развивать автомобиль. И ограничение это связано не с двигателем, а с автомобильной шиной.

Шина соприкасается с дорогой так называемой площадкой контакта. Действующие со стороны дороги силы, приложенные к шине в площадке контакта, представляют собой нагрузку, бегущую по шине.

Пневматическая шина (именно такие шины используются для автомобилей) представляет собой оболочку, «натянутую» внутренним давлением воздуха. Форма шины, как всем известно, близка к тороидальной.

Выделим мысленно малый элемент A оболочки шины (рис. 3). На этот участок со стороны соседей действуют силы натяжения, направленные вдоль параллели и вдоль меридиана (точнее, по касательным к ним). Пусть значения этих сил, отнесенных к единице длины (по параллели) и к единице ширины (по меридиану) элемента A , равны, соответственно, $|\vec{N}_x|$ и $|\vec{N}_y|$.

Анализ зависимости между этими силами и скоростью шины дает значение критической скорости. Формула для $V_{кр}$ в этом случае оказывается аналогичной формуле (3) для тяжелой ленты —

$$|\vec{V}_{кр}| = \sqrt{\frac{|\vec{N}_x|}{m'}} \quad (4)$$

— с той разницей, что здесь m' — масса единицы поверхности оболочки. Из формулы (4) видно, что критическая скорость тем больше, чем сильнее

растянута шина в направлении параллели.

Для увеличения прочности шины при изготовлении оболочки в качестве «арматуры» используют сетку из очень прочных нитей (корда). Иногда нити делают стальными (для шин грузовых автомобилей, которые должны выдерживать большие нагрузки). Чтобы оценить роль сетки-арматуры, достаточно сказать, что если бы ее не было, то шина «лопалась» бы при избыточных давлениях в 20—30 раз меньших, чем те, которые выдерживает современная шина с сеткой. (Для легковых автомобилей это давление 1,5—2 атм, для грузовых — 4—6 атм.)

Направление нитей корда характеризуется углом α . Значение критической скорости зависит от этого угла:

$$|\vec{V}_{кр}| = K \operatorname{ctg} \alpha.$$

Здесь K — коэффициент, определяемый давлением p воздуха в шине, радиусом r поперечного сечения шины и величиной m' :

$$K = \sqrt{\frac{pr}{m'}}.$$

Таким образом,

$$|\vec{V}_{кр}| = \sqrt{\frac{pr}{m'}} \operatorname{ctg} \alpha. \quad (5)$$

Это — так называемая формула Тарнера. Вы можете вывести ее самостоятельно, используя свое знание школьного курса физики.

Тем, кто решил задачу Ф514 (см. «Квант» № 5, 1978), сделать это просто. Для тех, кто не решал этой задачи, даем указания, которые помогут вывести формулу (5). Рассмотрите условия равновесия элемента A в предположении, что кривизна в на-

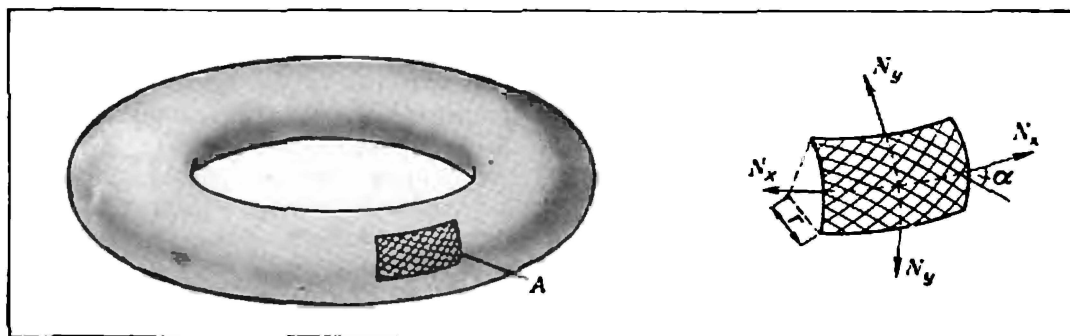


Рис. 3.