ВЫХОДИТ РАЗ В ДВЕ НЕДЕЛИ

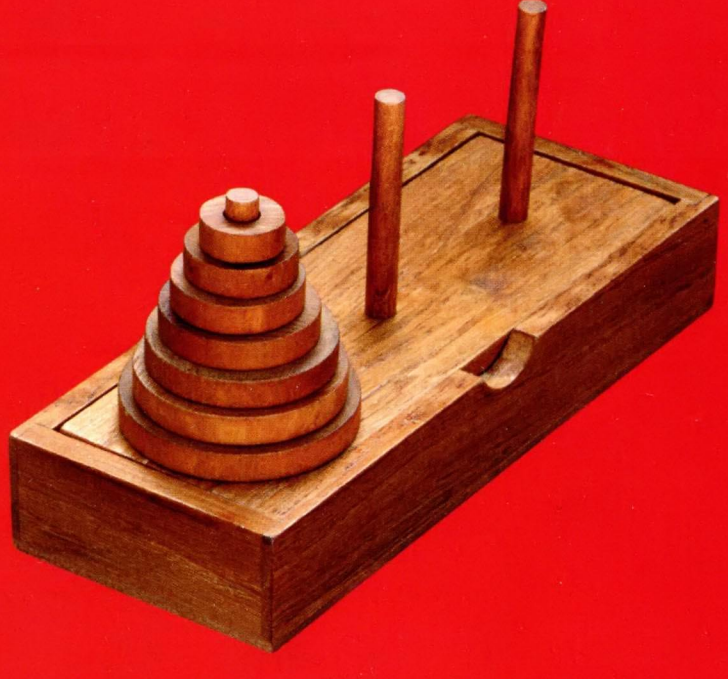
Рекомендуемая розничная цена: 279 руб.
Розничная цена: 49,90 грн, 990 тенге

Занимательные ГОЛОВОЛОМКИ

КОЛЛЕКЦИЯ ЛОГИЧЕСКИХ ИГР ОТ DeAGOSTINI

6

Ханойская башня



ISSN 2225-1782 00006
9 772225 178772

DeAGOSTINI

«ЗАНИМАТЕЛЬНЫЕ ГОЛОВОЛОМКИ»
Издание выходит раз в две недели
Выпуск № 6, 2012
РОССИЯ

ИЗДАТЕЛЬ, УЧРЕДИТЕЛЬ, РЕДАКЦИЯ:
ООО «Де Агостини», Россия
ЮРИДИЧЕСКИЙ АДРЕС: 105 066, г. Москва,
ул. Александра Лукьянова, д.3, стр.1
Письма читателей по данному адресу не принимаются.

ГЕНЕРАЛЬНЫЙ ДИРЕКТОР: Николаос Скилакис
ГЛАВНЫЙ РЕДАКТОР: Анастасия Жаркова
ФИНАНСОВЫЙ ДИРЕКТОР: Наталия Василенко
КОММЕРЧЕСКИЙ ДИРЕКТОР: Александр Якутов
МЕНЕДЖЕР ПО МАРКЕТИНГУ: Михаил Ткачук
МЛАДШИЙ МЕНЕДЖЕР ПО ПРОДУКТУ:
Любовь Мартынова

Свидетельство о регистрации средства массовой информации в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) ПИ № ФС77-43310 от 28.12.2010 г.

Для заказа пропущенных номеров
и по всем вопросам, касающимся информации о коллекции, заходите на сайт
www.deagostini.ru

по остальным вопросам обращайтесь по телефону бесплатной «горячей линии» в России:
8-800-200-02-01

Телефон «горячей линии» для читателей Москвы:
8-495-660-02-02

АДРЕС ДЛЯ ПИСЕМ ЧИТАТЕЛЕЙ:
Россия, 170100, г. Тверь, Почтамт, а/я 245,
«Де Агостини», «Занимательные головоломки»

РАСПРОСТРАНЕНИЕ: ЗАО «ИД Бурда»

УКРАИНА
ИЗДАТЕЛЬ И УЧРЕДИТЕЛЬ:
ООО «Де Агостини Паблишинг», Украина
ЮРИДИЧЕСКИЙ АДРЕС: 01032, Украина,
г. Киев, ул. Саксаганского, д. 119
ГЕНЕРАЛЬНЫЙ ДИРЕКТОР: Екатерина Клименко

Свидетельство о государственной регистрации печатного СМИ Министерства юстиции Украины КВ № 17502-6252Р от 01.03.2011

АДРЕС ДЛЯ ПИСЕМ ЧИТАТЕЛЕЙ:
Украина, 01033, г. Киев, а/я «Де Агостини»,
«Занимательные головоломки»
Україна, 01033, м. Київ, а/с «Де Агостіні»

Для заказа пропущенных номеров
и по всем вопросам, касающимся информации о коллекции, заходите на сайт
www.deagostini.ua

по остальным вопросам обращайтесь по телефону бесплатной «горячей линии» в Украине:
0-800-500-8-40

БЕЛАРУСЬ
Импортер и дистрибьютор в РБ ООО «РЭМ-ИНФО»,
г. Минск, пер. Козлова, д. 7г, тел.: (017) 297-92-75
АДРЕС ДЛЯ ПИСЕМ ЧИТАТЕЛЕЙ:
Республика Беларусь, 220037, г. Минск,
а/я 221, ООО «РЭМ-ИНФО», «Де Агостини»,
«Занимательные головоломки»

КАЗАХСТАН
РАСПРОСТРАНЕНИЕ: ТОО «КГП «Бурда-Алатау-Пресс»

РЕКОМЕНДУЕМАЯ РОЗНИЧНАЯ ЦЕНА: 279 руб.
РОЗНИЧНАЯ ЦЕНА: 49,90 грн, 990 тенге

ОТПЕЧАТАНО В ТИПОГРАФИИ: G. Canale & C. S.p.A.
Sos. Cernica 47, Bucuresti, Pantelimon – Ilfov, Romania.

ТИРАЖ: 240 000 экз.

Издатель оставляет за собой право изменять последовательность номеров и их содержание.

Издатель оставляет за собой право увеличить рекомендуемую цену выпусков.

Неотъемлемой частью каждого выпуска является приложение.

ISSN 2225-1782

ДАТА ВЫХОДА В РОССИИ: 24.04.2012

занимательные ГОЛОВОЛОМКИ

КОЛЛЕКЦИЯ ЛОГИЧЕСКИХ ИГР ОТ DeAGOSTINI

В этом выпуске:

Если в начале XX века криптология воспринималась как развлечение и атрибут дипломатических интриг, то к концу столетия она легла в основу принципа работы всех современных средств связи. Соответственно повысился уровень ее сложности и возросла доля математической составляющей.

Криптология

Тайны за семью печатями

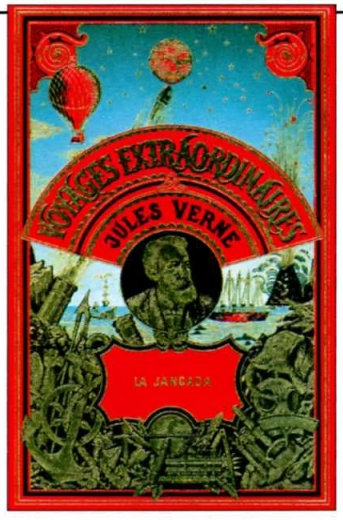
Для шифрования, как и для дешифровки, требуется особый склад ума. Например, такой, как у шахматистов: нужно одновременно и думать и о выборе подходящего алгоритма шифрования, и просчитывать, что предпримет противник, чтобы взломать шифр.

Основные методы

Два главных способа шифрования информации — это метод перестановок и метод подстановки. В первом случае буквы в сообщении остаются те же, но меняется их порядок. Путем перестановки букв составляется анаграмма, то есть новое слово (например, АРКА — КАРА). О методе шифрования посредством перестановок рассказывается в следующем разделе.

При использовании метода подстановки буквы заменяются цифрами, знаками или другими буквами; ответ на загадку, какая буква скрывается под каким знаком, содержится в ключе. Разновидностью этого метода является так называемый «шифр сдвига», известнейший пример которого — код Цезаря.

В целях повышения криптографической стойкости кода в одной системе шифрования вместе или по очереди могут использоваться и перестановки, и замена.



▲ *Роман Жюля Верна «Жангада» начинается с непонятной вереницы букв. Это криптограмма на основе метода перестановок, слово-ключ к расшифровке которой — ОРТЕГА. Поиск ключа занимает почти весь роман, но расшифровка спасает жизнь невиновного. Во времена Жюля Верна этот тип криптограмм был одним из самых популярных.*

Перестановки

Рассмотрим метод одиночной перестановки по ключу. Ключом выступает слово, которое должны знать и отправитель, и получатель. Например, если секретное слово «КОЛЛЕДЖ», то чтобы зашифровать сообщение:

УВИДИМСЯ В СЕМЬ У ТЕБЯ ДОМА,

нам нужно сделать следующее: пишем слово-ключ и под каждой его буквой подписываем номер в том порядке, в котором они стоят в алфавите: сначала «Д», затем «Е», «Ж» и так далее. Если какая-то буква повторяется, то нумерация идет слева направо.

К	О	Л	Л	Е	Д	Ж
4	7	5	6	2	1	3

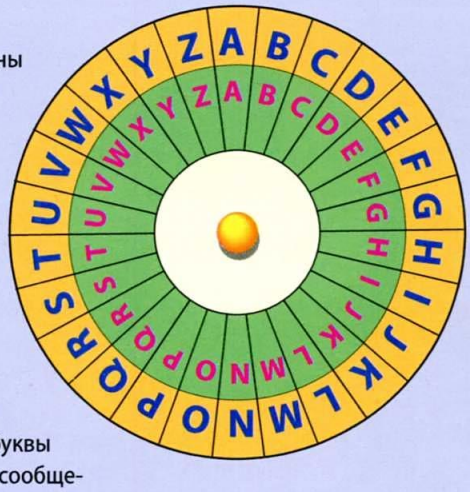
После этого текст сообщения без пробелов вписывается в таблицу под словом-ключом.

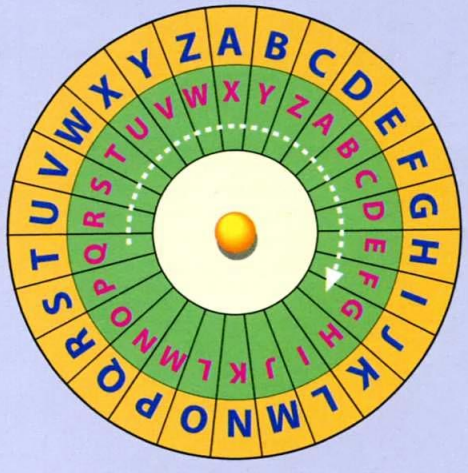
К	О	Л	Л	Е	Д	Ж
4	7	5	6	2	1	3
У	В	И	Д	И	М	С
Я	В	С	Е	М	Ь	У
Т	Е	Б	Я	Д	О	М
А						

Шифровальные диски

Для шифрования методом простой замены используются специальные шифровальные диски, которые можно сделать из картона. Необходимо вырезать два круга разного диаметра, написать по краю каждого алфавит, а затем скрепить их при помощи булавки или кнопки.

Здесь и отправителю, и получателю сообщения важно знать букву-ключ. Если ключом является буква «D» нижнего диска, то верхний надо повернуть таким образом, чтобы литера «A» встала прямо над ней. После этого меняем все буквы «открытого текста» (то есть шифруемого сообщения) на буквы с нижнего диска. Так, слово «MADRID» в закодированном виде станет «JXAOFA».





После заполнения таблицы («ящика») сообщение, которое мы собираемся отправить, пишется по колонкам в порядке нумерации. В первом столбце окажется «МЬО», во втором — «ИМД» и так далее. Готовая шифровка будет выглядеть так:

МЬО ИМД СУМ УЯТА ИСБ ДЕЯ ВВЕ

Чтобы расшифровать сообщение, нужно просто все вернуть на свои места, то есть поместить группы букв в соответствующие столбцы. Этот тип шифрования использовался в испанской армии вплоть до семидесятых годов прошлого века. Он предполагает и более сложные уровни: процесс может повторяться несколько раз с различными ключами, что значительно затрудняет криптоанализ.

Частота

Когда криптограмма достаточно длинная и достигает хотя бы 100 знаков, можно проанализировать статистику и составить таблицу частоты, с которой появляются определенные буквы. Знаки сортируются на более частотные и более редкие, и полученные таблицы сравниваются с частотой употребления данных букв в языке, на котором написана криптограмма. В испанском, например, самые используемые буквы — это «E» и «A»; если текст достаточно длинный, то буквы появляются в нем приблизительно в следующем соотношении:

E = 17%, A = 12%, O = 9%, L = 8%,
S = 8%, N = 7%, D = 7%...

Таким образом можно изучать и частоту первых и последних букв каждого слова, либо частоту групп из двух слов (да, но, по) и так далее.

В литературе встречается огромное количество примеров шифрования методом замены. Читатель может разгадать их только если знает частоту употребления различных букв и умеет быть внимательным. «Красный жук» — одна из самых известных повестей североамериканского писателя Эдгара Аллана По — содержит в себе загадочное зашифрованное сообщение, которое расшифровали благодаря статистическим техникам подсчета частоты употребления букв в английском языке. Но эта разгадка привела лишь к еще большей загадке.

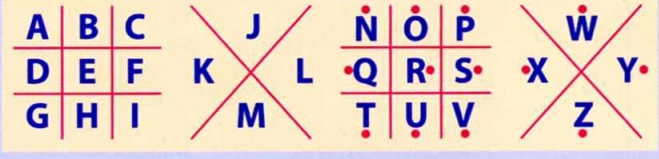
Шифр Виженера

Эта система была придумана французским дипломатом Блезом Виженером, родившимся в 1523 году. Преимущество данного метода заключается в том, что каждую букву можно закодировать двадцатью шестью различными способами — в основе алгоритма лежит таблица, включающая в себя 26 строчек с алфавитом, и каждая строка начинается со следующей буквы. Так, в алфавите №4 буква A заменяется буквой E, но при использовании алфавита №22 буква A станет буквой W. При условии замены номера алфавита в каждом сообщении шансы разгадать шифр по коду частоты сильно падают. Но дешифровка становится еще более сложной, если разные строки используются для шифрования букв одного сообщения. Например, шифровальщик может взять первую букву из строки №8, вторую — из алфавита №14 и так далее. В таких случаях получатель должен знать слово-ключ. Если в качестве ключа берется, допустим, слово LUIS, то в шифре используются строки, которые начинаются с этих букв, а именно: 8, 11, 18 и 20 — в восходящем порядке (от меньшего к большему).

	a b c d e f g h i j k l m n o p q r s t u v w x y z
1	B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
2	C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
3	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
4	E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
5	F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
6	G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
7	H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
8	I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
9	J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
10	K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
11	L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
12	M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
13	N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
14	O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
15	P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
16	Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
17	R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
18	S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
19	T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
20	U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
21	V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
22	W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
23	X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
24	Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
25	Z A B C D E F G H I J K L M N O P Q R S T U V W X Y
26	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Диаграммы

Замена букв сообщения на любые другие условные символы — это криптографический метод шифрования. Но следует иметь в виду, что его эффективность напрямую зависит от легкости составления и легкости расшифровки текста отправителем и адресатом. В то же время для тех, кто вне игры, алгоритм должен оставаться недоступным. Удобен в использовании метод, основанный на распределении букв алфавита следующим образом:



Размещение букв в сетке может быть произвольным. Важно чтобы и отправитель, и получатель владели одинаковыми ключами. Уже известная нам фраза «Увидимся в семь у тебя дома» (на испанском языке «NOS VEMOS A LAS SIETE EN TU CASA») будет выглядеть так:

Короткое сообщение, зашифрованное такими символами, расшифровать тяжело; взломать код, проанализировав частоту употребления знаков, удастся лишь в том случае, если шифровка содержит много слов.

ВОЕННАЯ КРИПТОГРАФИЯ

В первой половине XX века телефон, телеграф и радио были для высоких военных чинов жизненно-важными средствами связи. Но это было и слабое звено — ведь враг всегда мог перехватить информацию. Военным пришлось развивать криптографические системы и выводить их на самый современный уровень, особенно во время Второй мировой войны. Криптоанализ, в свою очередь, привлек все возможные математические и статистические ресурсы для дешифровки сообщений врага.

Язык индейцев навахо

Один из способов усложнить дешифровку сообщения — это использование языка, не имеющего письменности. Во время Второй мировой войны американцы для передачи устных сообщений на поле боя использовали индейцев племени навахо. Эта идея принадлежала Филиппу Джонстону, который говорил на языке навахо, так как вырос в резервации. Навахо очень сложный язык, его звучание представляет собой странное чередование назальных и гортанных звуков, которые почти невозможно записать. Отсутствие в языке навахо военных терминов компенсировали другими словами. Например, истребители назывались «колибри», разведчики — «филины», «бронированный» — «кит», «бомбы» — «яйца». Сотни названий живой природы. Еще одним явным плюсом данной системы связи являлась скорость передачи: связист тут же переводил сообщение на английский и в таком виде передавал информацию адресату, таким образом, никаких специальных усилий для шифрования и дешифрования предпринимать не приходилось. Благодаря индейцам навахо армия США на Атлантическом фронте имела совершенную систему связи: быструю и не поддающуюся ни дешифровке, ни фальсификации.

▼ *Два индейца племени навахо из Корпуса Морской пехоты США во время Второй мировой войны передают сообщение на языке навахо с острова в Тихом океане.*

JN-25 и Мидуэйское сражение

Код JN-25 использовался японской службой связи на протяжении всей Второй мировой войны. Располагавшаяся в Перл-Харборе станция «HYPO», которая находилась под командованием коменданта Джозефа Рокафорта, должна была данный код расшифровать, что само по себе имело решающее значение для хода военных действий. От этого зависело, смогут ли американцы переломить в свою пользу хрупкое равновесие военно-морских сил, начинавшее склоняться в пользу Японии. Код JN-25 состоял приблизительно из 45 000 пятизначных чисел, каждое из которых представляло слово или фразу. В момент передачи сообщения цифры дополнительно кодировались при помощи специальных таблиц с дополнительными

ЭТО ИНТЕРЕСНО

- Дешифровке японских сообщений американцы обязаны многими своими успехами во Второй мировой войне. Одним из наиболее значительных достижений стал захват японского командующего военно-морским флотом адмирала Ямамото по пути на Соломоновы острова. Адмирал Нимиц отправил на перехват 18 истребителей. Ямамото следовал точно по тому маршруту, который был указан в перехваченных шифровках.
- Шифровальное подразделение в Блетчли-парк с декабря 1943 года имело в своем распоряжении программируемую шифровальную машину «Колоссус», способную расшифровывать до 5000 знаков в секунду (ее можно считать одним из предков современных компьютеров). Когда война закончилась, машину уничтожили. Первым настоящим компьютером стал «ENIAC», собранный в 1946 году.

◀ *Немецкие солдаты во время Второй мировой войны шифруют сообщение на шифровальной машине «Энигма». Это портативное шифровальное устройство было достаточно компактно, чтобы носить его с собой и работать на нем непосредственно на поле боя.*

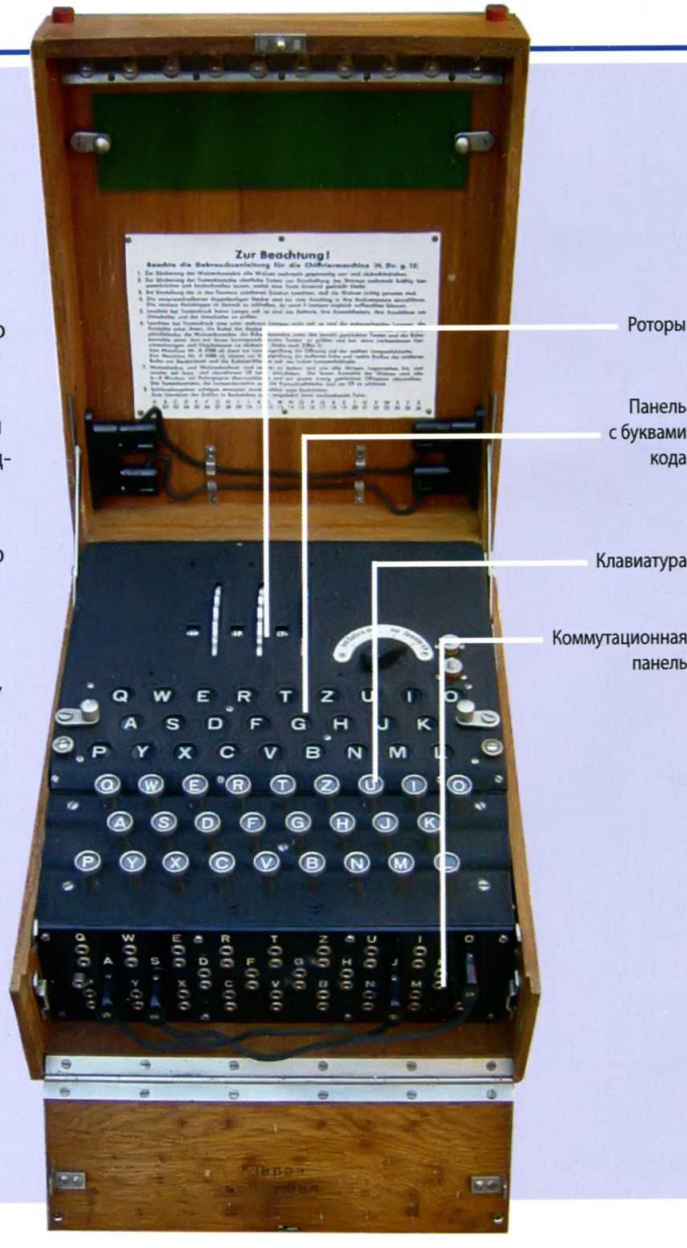
номерами. Чтобы разгадать этот код, нужно было посредством математического анализа найти первоначальные значения чисел, а затем статистическими методами проанализировать шаблоны повторения и таким образом вычислить значение каждого из пятизначных чисел. И июне 1942 года американцам удалось взломать шифр JN-25; в течение весны того же года были перехвачены несколько сообщений, по которым удалось вычислить скопление военно-морских сил, направляющихся к объекту, обозначенному как «AF». Специалисты станции «HYPO» уже расшифровали коды японцев, но эти две буквы продолжали оставаться загадкой. Тогда американцы отправили незашифрованное сообщение, в котором говорилось, что запасы воды на архипелаге Мидуэй серьезно загрязнены. Через некоторое время было перехвачено сообщение японских спецслужб, закодированное в JN-25, в котором говорилось: «AF остался без воды». Именно эта расшифровка и помогла адмиралу Честеру Нимицу победить в Мидуэйском сражении.

Шифровальная машина «Энигма»

Еще в 1926 году у немцев появилась шифровальная система, казавшаяся неуязвимой. «Энигма» очень похожа на печатную машинку, ее можно было использовать непосредственно на фронте, она не занимала много места на подводных лодках. «Энигма» состояла из трех основных компонентов, соединенных кабелями: во-первых, у нее была клавиатура, на которой сообщения печатались обычным текстом; нажатие клавиш приводило в движение специальный шифровальный механизм, состоявший из нескольких роторов; в результате на панели с подсветкой загоралась буква кода. Позже механизм был усложнен, и у машины появились рефлекторы и коммутационная панель, к которой подключались кабели, позволявшие менять местами буквы до прохождения сигнала через роторы. Перед началом работы шифровальщик устанавливал роторы в заранее условленную стартовую позицию, и таким образом задавалась определенная кодировка сообщений.

Несмотря на то, что у разведслужб союзников были машины «Энигма» и даже некоторые книги с кодами, количество шифров, производимых машиной (около 17 триллионов), делало дешифровку почти невозможной. Уже после начала Второй мировой войны для дешифровки кодов «Энигмы» сверхсекретная британская Правительственная школа кодов и шифров, находящаяся в Блетчли-парке, собрала в своих стенах сотни математиков, лингвистов и ученых под руководством Алана Тьюринга, профессора математики Кембриджского университета.

Усложняло расшифровку сообщений «Энигмы» то, что немцы ежедневно меняли коды. Из-за этого каждое утро начиналось в Блетчли-парке с поиска слова «Wetter» (погода), так как первые сообщения немцев имели отношение к погоде. К концу 1941 года благодаря сочетанию интуиции, удачи, средствам связи и дешифровальным машинам «Бомба», созданным Тьюрингом, немецкие сообщения перестали быть недоступными для союзников.



ГРАЖДАНСКАЯ КРИПТОГРАФИЯ

Некоторое время назад, после массовой компьютеризации современного общества, криптография перестала быть прерогативой военных и дипломатов. Теперь она используется в самых разных сферах жизни гражданского общества. Банкам необходимо защищать свои данные; абоненты мобильной связи требуют, чтобы их телефонные разговоры не прослушивались; медицинские, статистические, избирательные базы данных обязаны надежно хранить секреты своих пользователей; для проведения операций по кредитным картам или доступа в локальные компьютерные сети необходим персональный пароль, и уже не за горами тот день, когда «электронный нотариус» начнет использовать для заверения сделок цифровую аутентификацию. Все это требует широкого и специализированного использования криптографии. Понимаем мы это или нет, но мы живем в мире тайн, защищенных в большей или меньшей степени.

В современной криптографии процесс шифрования полностью компьютеризирован, и все механизмы шифрования находятся внутри маленьких чипов. Пользователю остается только набрать текст на компьютере, который сам сделает все остальное. Есть два типа ключей, используемых в криптографических программах: симметричное шифрование и асимметричное, или открытое шифрование.

Симметричное шифрование

Системой симметричного шифрования называется система, использующая один и тот же ключ и для кодификации, и для декодификации информации. Например, в коде Цезаря необходимо прибавить три буквы, чтобы зашифровать сообщение, и отнять три, чтобы расшифровать — два противоположных действия, но с одинаковым ключом. Преимущество этого метода состоит в том, что благодаря своей быстроте он очень практичен при работе с большими объемами информации. Но, несомненно, есть и минусы, и главный из них — проблема распределения кодов: когда постоянно используется один и тот же канал связи, то в качестве меры безопасности необходимо с определенной частотой менять коды. Это предполагает распределение новых кодов по тому же каналу связи или посредством передачи сообщений, что ставит под угрозу всю систему. Второй минус — необходимость установления подлинности личности отправителя, ведь если кто-то расшифрует ключ, то сможет посылать сообщения от чужого имени.

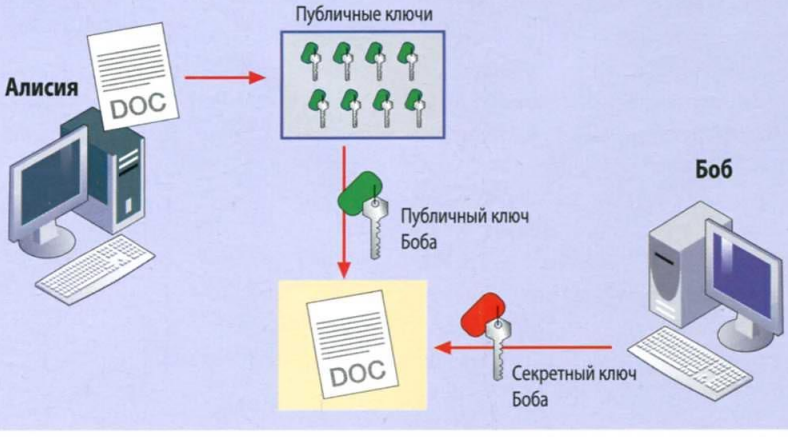
Открытое шифрование

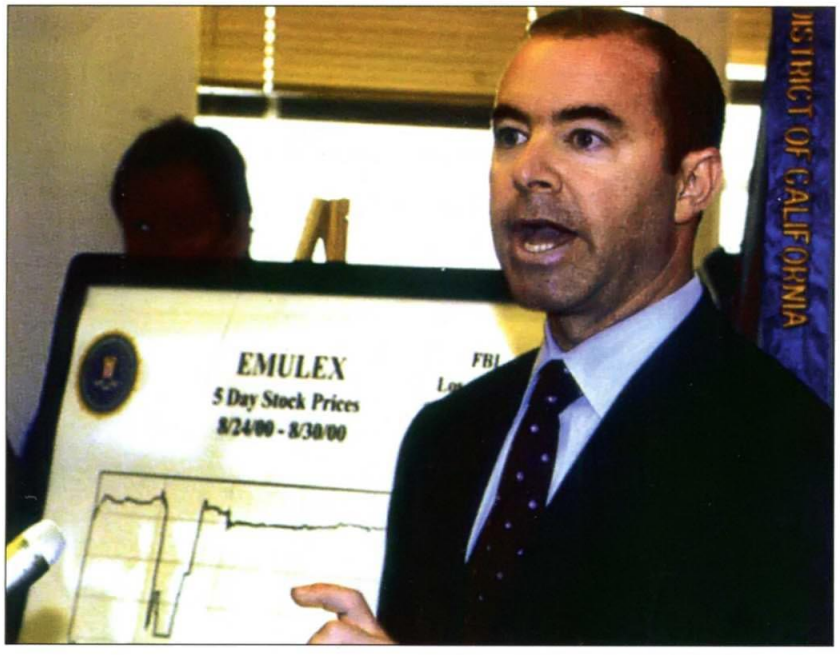
В 1975 году У. Диффи и М. Хеллман из Стэнфордского университета разработали концепцию открытого шифрования, или публичных ключей. Данная система базируется на определенных математических принципах, которые называются односторонними. Они допускают шифрование публичным ключом, но не допускают дешифрования, если неизвестен секретный ключ. Идея этого алгоритма состоит в том, что у каждого пользователя есть два ключа: публичный и секретный. Если пользователь хочет отправить сообщение Хуану, то зашифровывает сообщение публичным ключом, известным не только Хуану, но и любому другому человеку.

▲ *Сложность современных процедур шифрования во многих случаях делает расшифровку возможной только лишь с помощью суперкомпьютеров — таких как, например, CRAY-1 на фото.*

Как работают публичные ключи

Когда Алисия хочет отправить документ Бобу, она заходит на сайт, на котором, как на брелоке, висят ключи. Алисия берет публичный ключ Боба и шифрует документ — словно опускает свое письмо в ящик и закрывает его специальным ключом (зеленым), которым можно только закрывать. С этого момента ящик может открыть только Боб и только своим красным ключом, который есть лишь у него.





▲ *Способности некоторых «хакеров» позволяют взламывать защитные коды крупных компаний. Порою такие преступления кажутся совершенно невероятными. На фото генеральный прокурор Лос-Анджелеса объясняет, как 23-летний студент получил на бирже 241 000 долларов и при этом заставил компанию Emulex потерять 2200 миллионов, отправляя ложные сообщения от ее имени.*

ЭТО ИНТЕРЕСНО

- В апреле 1994 года сумели «разложить» 129-значное число, известное под названием RSA-129. Группа из 600 математиков и 1600 волонтеров смогла факторизовать его, то есть поделить на простые числа. Однако посчитано, что если заставить работать одновременно все компьютеры в мире, то для факторизации числа, состоящего из 1024 знаков, понадобится время, равное возрасту Вселенной (15 миллиардов лет).
- Компании, производящие программное обеспечение, хранят секретные ключи на жестких дисках в форме таблеток, которые имеют очень сложную систему защиты. Если такую таблетку открыть неправильно, и в нее попадет кислород, все содержимое сплавится в однородную массу. А при попытке просветить рентгеном все данные превратятся в нули.

Однако только у Хуана есть секретный ключ, которым он может расшифровать это сообщение. У данного способа есть огромный плюс — секретный ключ Хуана никогда не попадает в открытый доступ, что позволяет долгое время его не обновлять.

Математические основы

Существует несколько алгоритмов (математических методов), разрешающих использование открытого ключа. Самый известный — это RSA, разработанный Райвестом, Шамиром и Адлеманом в 1977 году. В основе его лежит принцип факторизации числа как произведения двух простых чисел. Вспомним, что простое число — это такое число, которое делится на себя и на единицу, как 3, 5, 7, 11 и так далее. Если взять два таких числа, например, 7 и 19, и умножить их друг на друга, то получится 133. Число 133 будет в этой системе открытым ключом, а 7 и 19 — это секретный ключ. Ясно, что чем больше число, тем сложнее найти два простых множителя, на которые оно будет разлагаться. В случае с числом 527 потребуется больше попыток (а множители в данном случае 17 и 31). Таким образом, взломать код может тот, кто способен обнаружить в открытом ключе два простых числа. То есть, если в криптографической системе известный всем открытый ключ 22, то тот, кто сможет разгадать, что $22 = 11 \times 2$, сможет взломать код.

Нетрудно догадаться, что коды, из которых состоят эти ключи, не такие уж и легкие. В наших примерах использованы числа из двух или трех цифр, но в реальности открытый ключ обычно состоит из чисел в 128, 1024 и больше знаков (например, современные военные ключи обычно состоят из 2048 цифр). Чем больше знаков в системе, тем устойчивее к атакам она будет. Однако на расшифровку в этом случае требуется больше времени.

Применение криптографии

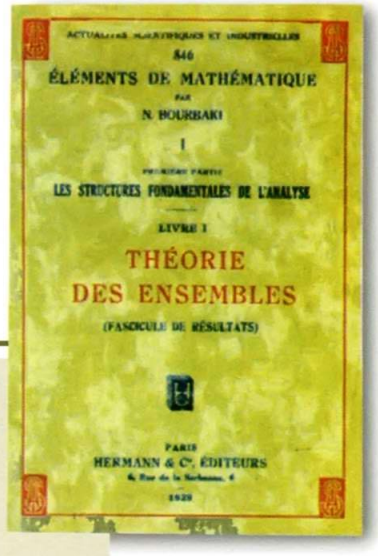
В настоящее время криптография присутствует во многих аспектах повседневной жизни, хотя не всегда ее можно заметить невооруженным глазом. Такие явления, как мобильная связь, платное телевидение или интернет-коммерция (справа) не были бы возможны без применения криптографических методов, позволяющих гарантировать безопасность и неприкосновенность данных. У электронных голосований также есть проблемы с безопасностью, и криптография необходима для сохранения тайны голосования и для того, чтобы голосовать могли только зарегистрированные пользователи и только единожды.

Николя Бурбаки — один из самых знаменитых математиков XX века. На его счету — пересмотр основ математики и спорная образовательная реформа. Хотя на самом деле никогда не существовало ученого по фамилии Бурбаки.

Секретное математическое общество
Николя Бурбаки

◀ *Члены группы Бурбаки на своем съезде в г.Шансе в 1937 году.*

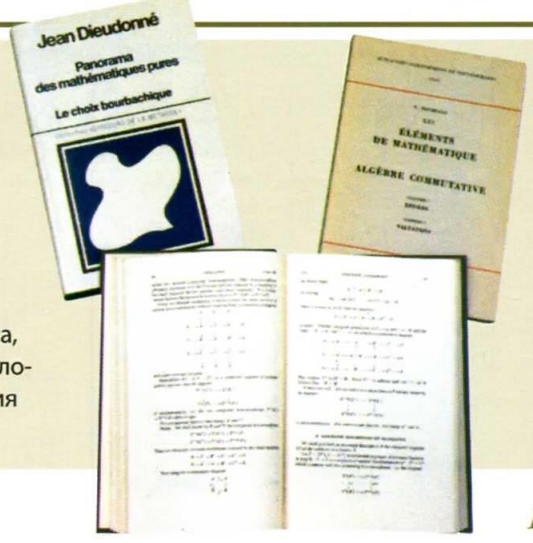
Математики Анри Картан и Андре Вейль, читавшие в Страсбургском университете курсы по дифференциальному и интегральному исчислению, не раз спорили о необходимости реформы преподавания математики в университетах. Но для этого сначала нужно было написать хороший обобщающий труд по математическому анализу, который можно было бы использовать как учебное пособие, а затем стандартизировать по нему обучение. В конце 1934 года Вейль сообщил Картану, что он с еще пятью или шестью друзьями хотел бы собраться для совместной работы над этим проектом. Так, совершенно неожиданно для всех, родилась группа Бурбаки. Книга, которая начиналась как простой учебник математического анализа, в итоге превратилась в монументальный труд с амбициозным названием «Элементы математики» (в оригинале «Начала математики»). Члены группы (или «банды», как им нравилось себя называть) брали на себя обязательство привести царицу наук в определенный порядок. На основе концепции целостности они хотели посредством ряда аксиом возвести здание новой математики. Это была бы, без сомнения, чистейшая математика, абстрактная, без лишней информации (например, геометрии, по их мнению, вообще было не место среди математических наук).



▲ *Первый том «Теории множеств».*

Порядок в математике

Вот некоторые из последних публикаций группы Бурбаки. Самая важная из работ — «Элементы математики»; первый выпуск этого монументального труда, в котором более семи тысяч страниц, вышел в 1939 году, а последний — в 1998. Его целью было упорядочить мир безудержного математического прогресса, создать четкий и единый язык, строгие и логичные правила игры и базис для развития современной математики.



И строго, и с улыбкой

Собралась группа лучших математиков своей эпохи. Собралась бескорыстно, не ради карьеры, без какого-либо желания прославиться. Именно это и побудило их спрятаться за псевдонимом Николя Бурбаки. Группа не была большой и периодически обновлялась; одним из главных условий членства был возраст: по достижении 40 лет участник был обязан покинуть «банду». Прекрасный математический стиль, поразительное чувство юмора и хорошие связи с издательством «Hermann» — вскоре молодые ученые стали настоящим мифом. Н. Бурбаки превратился в магистра тайных знаний, число его последователей стремительно росло. Поначалу годы Бурбаки подписывал свои работы как Н. Бурбаки. Имя Николя он получил с первой работой, представленной в Академию Наук в 1935 году. Фамилию «Бурбаки» участники «банды» выбрали потому, что им слышалось в ней что-то русское, хотя на самом деле она была греческой.

◄ *Человек по фамилии Бурбаки (1816—1897) существовал на самом деле. Им был француз греческого происхождения, генерал, участвовавший во многих военных кампаниях франко-прусской войны под командованием Наполеона III. Бурбаки дослужился до звания командующего королевской гвардией. Похоже, наша группа математиков взяла эту фамилию в память о какой-то юношеской шутке.*

Любопытно, что Бурбаки подписывал свои книги как член Академии наук Полдавии и профессор Университета Нанкаго. Полдавии не существует ни на одной карте, а Нанкаго — это акроним, состоящий из названий городов Нанси и Чикаго.

Смерть Бурбаки

Хотя группа продолжает собираться три раза в год, последняя публикация увидела свет в 1998 году (предыдущая — в 1983). 1998-ой для многих является годом смерти Н. Бурбаки. Даже некоторые представители французской прессы осветили это в своих изданиях (Le Monde, Eureka, Libération...). Причин у этого заявления о смерти может быть множество. Но, вероятно, важнейшая из них лежит в самой природе математики. За последние годы математическая наука претерпела глобальные изменения, появились совершенно новые направления, методы, гипотезы, ускорился темп научной жизни. Во время расцвета Бурбаки количество публикаций по математике было близко к 3000 в год, в настоящее время их более 100000 за тот же период. Бурбаки опередил свое время, но время оставило его в прошлом.

▼ *В кафе «A. Capoulade», находящемся в Латинском квартале Парижа, Бурбаки собирались на свой первый съезд. Сейчас в этом заведении находится ресторан быстрого питания.*

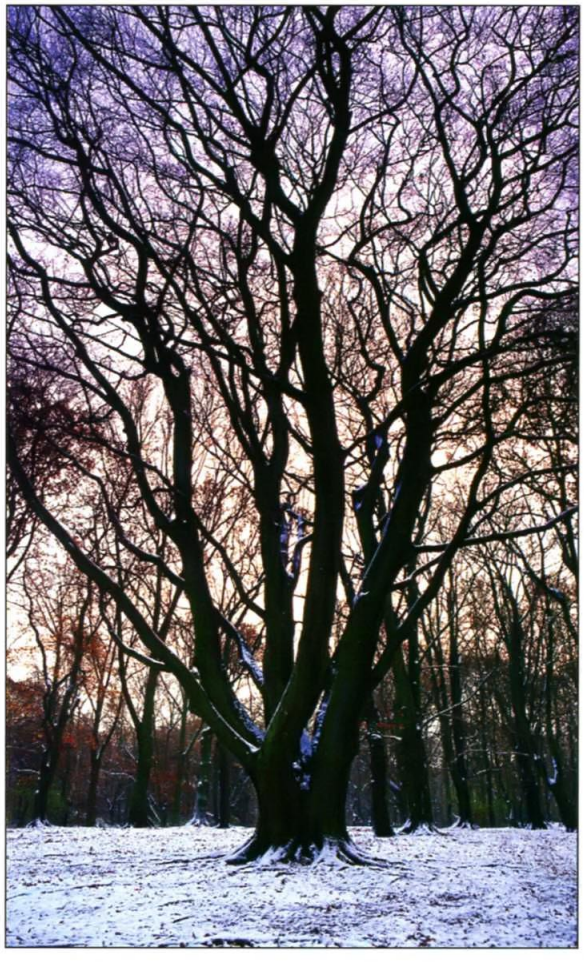
ЭТО ИНТЕРЕСНО

- На одном из своих съездов группа Бурбаки обсуждала некую очень серьезную тему, предложенную А. Картаном. В какой-то момент кто-то крикнул «Бум!». Это восклицание было перенято всеми членами группы. Со временем стало забываться, откуда взялся термин «бумология», используемый в определенных математических кругах.
- Однажды осенним утром 1948 года Анри Картану позвонил некий Николаидес Бурбаки. Сначала ученый подумал, что это нелепый розыгрыш, но на том конце провода находился торговый атташе посольства Греции в Париже, который был очень сердит: в интеллектуальных кругах Греции ходили слухи о том, что кто-то решил воспользоваться его именем. Картан встретился с атташе и объяснил ему ситуацию. С этого момента господин Николаидес Бурбаки стал частым гостем на приватных ужинах, организуемых группой после своих съездов.
- Американский математик Ральф Боас написал в «Британскую энциклопедию» небольшую заметку, в которой утверждал, что математика Н. Бурбаки не существует, это псевдоним. Чтобы отомстить, Бурбаки пустил слух, что математика Боаса не существует, и «Боас» — это всего лишь акроним, используемый редакцией журнала «Математикл Ревью».

Фрактальная геометрия — это причудливые, прекрасные, порою невидимые глазу природные формы, для которых не существует классических канонов. Нам не хватает математических знаний, чтобы «разгадать» эти фигуры, каждый элемент которых стремится к нулю.

Фракталы

Удивительные законы природы



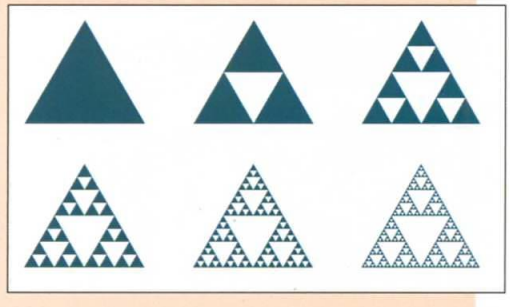
◀ *Один из самых ярких примеров фрактальной формы, данных нам природой. Ветви всегда сохраняют морфологическую структуру всего дерева.*

▶ *Программы для создания фракталов генерируют разноцветные фигуры немыслимой красоты.*

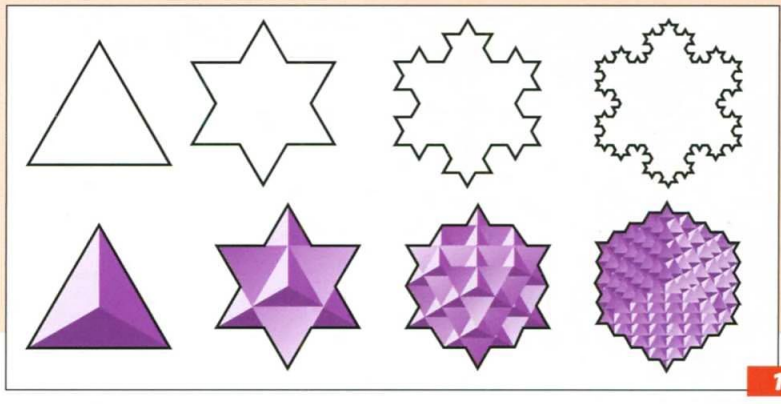
Фракталы были открыты в какой-то степени случайно. Бенуа Мандельброт работал на компьютере с итерированными функциями, и в какой-то момент заметил множество, названное впоследствии его именем. Итерированная функция — это, например, процесс, который мы создаем, если берем любое число, допустим, 3, возводим его в квадрат и прибавляем единицу. Получается 10. А сейчас делаем все то же самое с числом 10 — умножаем его на само себя и прибавляем единицу. Результат получается равен 101. И так далее. То, что делал Мандельброт, было очень похоже на это. Когда компьютер выдал графическую презентацию результатов, на экране появилась странная черно-белая фигура любопытной формы. При ее увеличении оказалось, что линия границы множества, казавшаяся ровной, на самом деле состоит из множества маленьких луковичных головок, каждая из которых повторяет форму оригинальной фигуры.

Геометрическое поколение фрактала

Некоторые фракталы генерируются геометрическим путем, при этом можно обойтись без компьютера. Один из самых простых фракталов — это так называемый треугольник Серпинского (рядом), который получается из равностороннего треугольника, внутри которого чертится другой треугольник, углами упирающийся в середины его сторон. Этот процесс повторяется несколько раз.



Из этого же треугольника при делении каждой стороны на три одинаковые части получается фрактал в виде звезды (внизу). Этот фрактал носит название «снежинка» или кривая Коха.



◀ *Польский математик Бенуа Мандельброт (1924—2010). С помощью компьютера Мандельброт, работавший в тот момент в «IBM's Watson Research Cente», графически представил достаточно простую функцию. Ученый и не думал, что открытый им феномен станет самым известным множеством в истории и объектом сотен исследований. Прошло уже достаточно много лет, но о множестве Мандельброта известно по-прежнему очень мало. Вычисления Б. Мандельброта были опубликованы в книге «Фрактальная геометрия природы» (1982).*

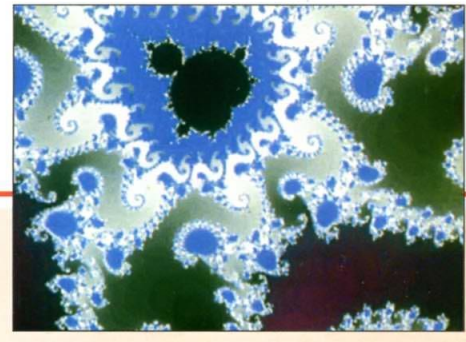
Что такое фрактал?

Математическое определение фрактала достаточно сложно, но, конечно же, опираясь на два самых характерных признака, можно дать ему интуитивное определение. Во-первых, фрактал обладает структурой самоподобия, то есть состоит из множества частей, каждая из которых подобна всей фигуре целиком. Чтобы получить макет фрактала, можно поставить вертикально ветви деревьев — издалека они будут похожи на сами деревья. Это происходит потому, что деревья обладают структурой самоподобия, которая присуща и фракталам. Вторая особенность фракталов заключается в том, что, несмотря на конечность своего объема, они парадоксальным образом имеют бесконечный периметр. Если мы попробуем измерить длину этой кривой, то обнаружим, что сколько бы мы ни увеличивали масштаб, пытаясь найти ровные «измеряемые» участки, из-за фундаментального свойства самоподобия мы будем видеть вместо этого все новые и новые изгибы. Математики конца XIX века называли эти красивые множества «математическими монстрами»; их характеристики фактически не имеют ничего общего с классической евклидовой геометрией.

Применение

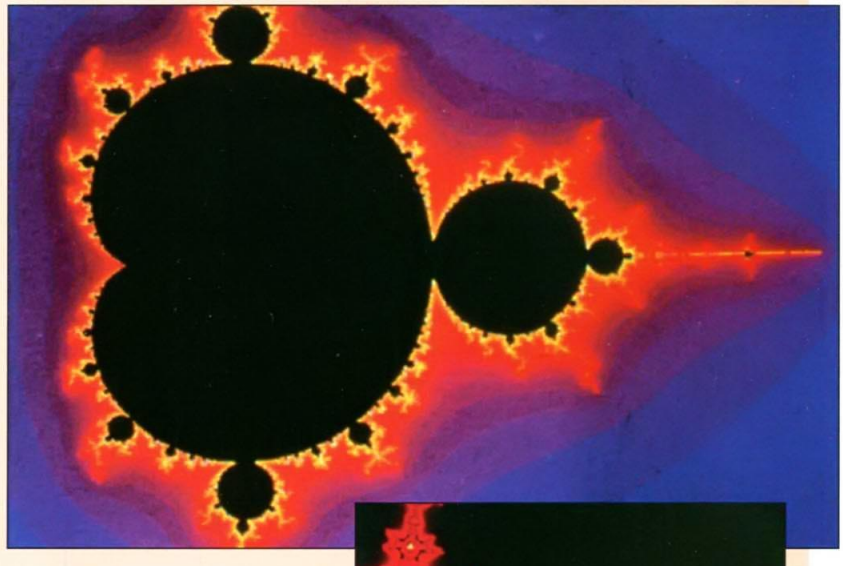
В человеческом теле также присутствуют фрактальные структуры: например, легкие. В грудной клетке они размещаются очень компактно, но если разложить этот важный орган человеческого организма на плоскости, то в таком виде он займет почти целую площадку для игры в сквош. В настоящее время также ведутся медицинские исследования фрактальной структуры остеопороза — дегенеративного заболевания костной структуры. Возможно, это позволит прерывать развитие болезни на начальном этапе.

А в музыкальном мире появился новый вид мелодий — «фрактальная музыка», которую создают при помощи компьютера: каждой точке и цвету множества дается определенное музыкальное значение. И хотя подобные композиции пока испытывают проблемы с ритмом, но уже в ближайшем будущем мы сможем слушать настоящие симфонии, рождающиеся благодаря множествам Жюлиа...



Множество Жюлиа

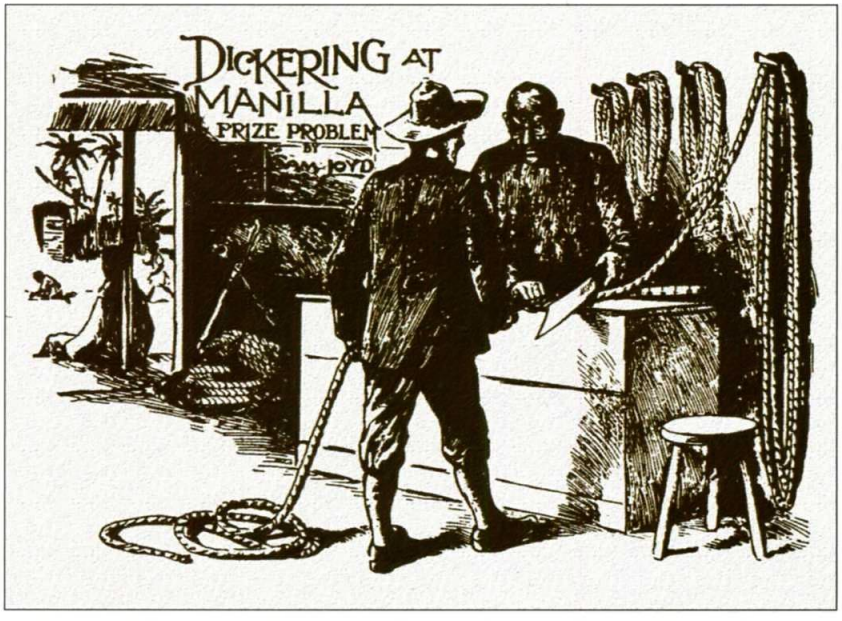
Это множество, напоминающее береговую линию острова, называется множеством Жюлиа в память о французском математике Гастоне Жюлиа, который вместе с Пьером Фату первым занялся изучением феномена фракталов. Математическая формула, используемая для создания множества, очень проста, но получающаяся фигура полна сюрпризов. При увеличении раскрывается целый сложный мир, заключенный в линию контура.



Подробнее на сайтах:

http://www.uvm.edu/~msargent/main.htm
Различные программы для создания фракталов.

http://sprott.physics.wisc.edu/fractals.htm
Бесплатные программы и галереи фракталов разных видов.



1. Торг в Маниле

Торговля манильской пенькой или канатами — основной бизнес на Филиппинах, и по большей части его контролируют экспортеры — китайцы, которые отправляют корабли с грузом пеньки во все части света. Японские мелкие торговцы славятся своеобразной манерой ведения бизнеса. Особенно своего собственного бизнеса. В отсутствии установленной валюты и фиксированных цен на товар каждая сделка превращается в состязание.

Следующая задача иллюстрирует обычный способ совершения сделки. Опустив простонародный язык, скажем, что китайский моряк заходит в лавку, торгующую канатами, и спрашивает:

— Не могли бы вы подсказать мне хорошую лавку, где можно купить качественный канат?

Лавочник-японец, проглотив скрытое оскорбление, отвечает:

— У меня только лучшие канаты. Но и самые худшие из тех, что у меня есть, наверняка будут лучше тех, которые вы ищете.

— Покажите мне лучшее, что у вас есть! Чтобы мне этого хватило, пока я не найду что-нибудь получше. Сколько вы берете за толстый канат?

— Семь долларов за бухту в сто футов длиной.

— Это слишком много и дорого. Я никогда не плачу больше доллара за хороший канат, а этот весь гнилой.

— Нормальный канат,— отвечает торговец,— показывая на бухте нетронутую печать, гарантирующую длину и качество.— Если у вас мало денег, то возьмите сколько вам нужно по два цента за фут.

— Отрежьте двадцать футов,— говорит моряк и хвастливо вытаскивает золотую пятидолларовую монету, демонстрируя свою платежеспособность.

Торговец с подчеркнуто сосредоточенным выражением лица отмеряет двадцать футов — моряк должен увидеть, как он старается все точно отмерить. Матрос, однако, говорит, что мерило, в котором должен быть один ярд, на самом деле на три дюйма короче, так как разметка прерывается на отметке в тридцать три дюйма. Таким образом, когда канат уже отрезан, моряк показывает на более длинную его часть и говорит: «Я заберу эти 80 футов. Нет, не надо мне посылать, я сам унесу». Затем бросает фальшивую монету в пять долларов, и торговцу приходится идти разменивать ее в соседнюю лавку. Получив свою сдачу, моряк уходит и забирает канат.

Задача состоит в том, чтобы сосчитать, сколько потерял торговец, если предположить, что ему придется заменить фальшивую монету настоящими деньгами и что канат действительно стоит два цента за фут. (Помните, что 1 ярд равен 36 дюймам, а 1 фут — 12 дюймам.)

2. Каков доход?

Один торговец продал велосипед за 50 долларов, затем выкупил его обратно за 40 и выиграл таким образом 10 долларов. Итак, у него есть велосипед и 10 долларов. Затем он снова продает велосипед, но уже за 45 долларов, выиграв еще 5 долларов, в общей сумме — 15.

— Но как же так,— воскликнет бухгалтер,— сначала у человека есть велосипед за 50 долларов и после второй продажи у него только 55 долларов! Каким образом он мог выручить больше пяти? Продажа велосипеда за 50 долларов — это просто обмен, который не предполагает ни доходов, ни расходов, но когда он покупает за 40 и продает за 45, то доход составляет 5 долларов, и это все.

— Я утверждаю,— возразит счетовод,— что когда велосипед продается за 50 долларов, а покупается обратно за 40, то чистый доход получается 10 долларов, потому что это один и тот же велосипед и к нему еще 10 долларов. Но когда он продает его за 45 долларов, то это уже просто обмен, о котором мы говорили, который не подразумевает ни потерь, ни доходов. Но это не влияет на его первый доход, и в итоге получается, что он выручил именно 10 долларов.

Это очень простая задача, и даже ученик первого класса мог бы решить ее в уме. Но тем не менее, у нас получилось три разных варианта ответа! Как вы считаете, какой из них верный?

3. Лавка старьевщика

Описывая посещение лавки старьевщика, Смит рассказал, что потратил там половину своих денег за полчаса таким образом, что у него осталось столько центов, сколько долларов было раньше, и половина долларов от центов, что были раньше. Итак, сколько потратил Смит?

4. Продажа кур

Фермер с женой на рынке хотели обменять живую птицу на скот из расчета, что восемьдесят пять кур равны одной лошади и одной корове. Предположительно, пять лошадей стоят столько же, сколько двенадцать коров.

— Джон,— сказала супруга,— давай возьмем еще столько же лошадей, сколько мы уже выбрали. Тогда у нас будет семнадцать лошадей и коров, которых нужно будет содержать во время зимы.

— Думаю, нам нужны еще коровы,— ответил муж.— Более того, думаю, если мы удвоим количество коров, которых выбрали, то у нас будет 19 голов коров и лошадей и точное число кур для обмена.

Эти простые деревенские жители не знали, что такое алгебра, но, разумеется, знали, сколько кур у них было и какое количество лошадей и коров они могли выручить.

Попросим наших эрудированных читателей, опираясь на данные из вышеизложенного диалога, посчитать, сколько кур привезли на рынок фермер с женой.

5. Алмазы и рубины

Стоит знать, что стоимость одного карата алмаза умножается на вес камня в квадрате, а стоимость карата рубина — на его вес в кубе. Например, если алмаз превосходного качества весом в один карат стоит 100 долларов, то камень весом в два карата будет стоить уже 400 долларов; а камень в три карата, соответственно, 900 долларов. Если качественный восточный рубин весом в один карат стоит 200 долларов, то двухкаратный камешек будет стоить уже 1600 долларов.

Один известный коммерсант, осваивающий алмазные шахты в Бразилии, Капской колонии и в других точках земного шара, показал мне два кольца с бриллиантами, которые обменял на два алмаза разных размеров, а как мы уже знаем, один карат стоит 100 долларов. Могли бы вы отгадать, какого размера были те камни, за которые коммерсант получил два кольца одинаковой формы? Конечно, есть много ответов, а потому мы бы попросили вас вычислить наименьший возможный размер для двух одинаковых камней, эквивалентный стоимости двух камней разного размера, но без необходимости их дробить.

Ответы

1. Первые 18 футов каната, которые отмерил торговец, на 3 дюйма на каждый ярд короче, или всего полтора фута меньше. В двух последних футах ничего не теряется, так как мерило обрезано только с одной стороны. Таким образом, торговец отдает моряку канат длиной в 81 фут с половиной, что по 2 цента за фут составляет 1,63 доллара. Стоимость этого куска получается 1,60 доллара (80 футов по два цента за фут), которые ему оплачивают фальшивой монетой в 5 долларов. Торговец дает моряку сдачу 3,40 доллара. Если мы прибавим эту сумму к 1,63 доллара — потере за канат, то общая потеря составит 5,03 доллара. А то, что сосед поменял ему фальшивые деньги, не имеет отношения ни к его доходам, ни к потерям.

2. Мы не знаем, сколько коммерсант заплатил за велосипед изначально. Так как этот момент неизвестен, то и ответ на данную задачу не может быть однозначным.

3. Смит начал с суммы в 99,98 долларов и потратил 49,99 доллара.

4. В загадке про кур любому фермеру ясно, что корова стоит 25 кур, а лошадь — 60. Фермер и его жена уже выбрали 5 лошадей и 7 коров, чья общая стоимость равна 475 курам. У них остается достаточно кур, чтобы купить еще 7 коров. $7 \times 25 = 175$, и в результате получается 650 кур.

5. Камень каждого кольца имел 5 каратов, потому каждое из них стоило по 2500 долларов, что в сумме равно 5000 долларов за два кольца. Размеры алмазов были в 1 и в 7 каратов (по цене 100 и 4900 долларов соответственно), что в итоге давало сумму, равную 5000 долларов.

Ханойская башня — это простая, но немыслимо красивая головоломка, которую могли бы изобрести тысячи лет назад. Но придумал ее французский математик Эдуард Люка в 1883 году.

Игра конца света
Ханойская башня

Легенда повествует о большом храме Варанаси, где под куполом, символизирующем центр мира, находится бронзовый диск, а на нем укреплены 3 алмазных стержня высотой в один локоть и толщиной с пчелу. На один из этих стержней во время создания мира бог Брама нанизал 64 диска из чистого золота, причем так, что каждый меньший диск лежит на большем, а самый большой — на бронзовом диске. Это и есть башня Брамы. Монахи в храме день и ночь занимаются тем, что перекладывают диски так, чтобы меньший диск никогда не оказывался под большим.

Как только все 64 диска будут переложены со стержня, на который бог Брама нанизал их при творении мира, на другой стержень, башня вместе с храмом обратятся в пыль, и под громовые раскаты погибнет мир.

В любом случае, пока не стоит слишком волноваться, потому что даже предположив, что работа ведется быстро, монахам придется проделать как минимум 18 446 744 073 709 551 615 движений.

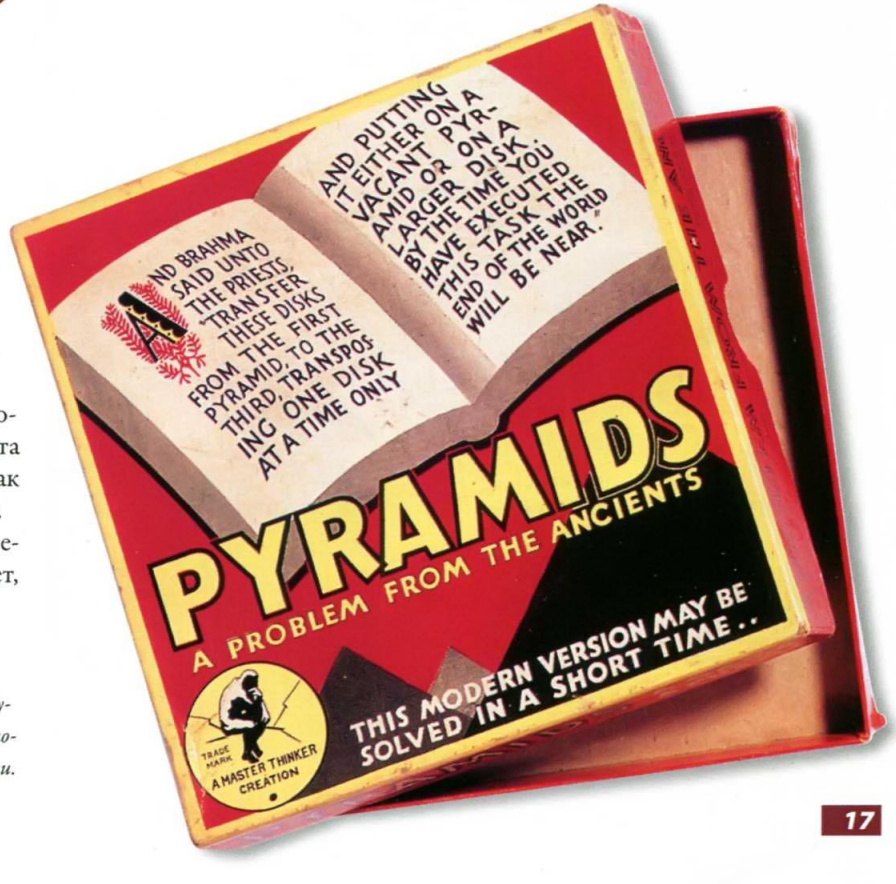
Даже если они будут делать по движению в секунду, им понадобится около 600 миллиардов лет, чтобы закончить.

Немного истории

На самом деле, эта головоломка была придумана французским математиком Эдуардом Люка, который представил ее общественности в 1883 году под названием «Ханойская башня». Как было написано на оригинальной упаковке, головоломку привез из Тонкина профессор Н. Клаус из Сиама, мандарин колледжа Ли Су Цян. Но и это оказалось игрой слов, анаграммой из слов «Люка из Дамьена, из школы Сан-Луи», где он был учителем.

Легенда о Храме в Варанаси была придумана Люка с целью заинтересовать публику.

◀ *В какой-то степени, очарование игры состоит в том, чтобы представлять себе легенду о башне Брамы с ее золотом, бриллиантами и концом света в момент разрешения головоломки. Сложность игры удваивается каждый раз, когда на стержень добавляется диск, и с 64 дисками игра становится практически бесконечной.*



▶ *Игра справа — это копия Ханойской башни, названная «Пирамида» и вышедшая на рынок в 1929 году; головоломка Эдуарда Люка всегда имела колоссальный успех. Существует множество ее «клонов» под другими названиями.*

В чем заключается игра

В классической версии игра состоит из подставки с тремя стержнями, на одном из которых нанизано определенное количество дисков разного размера, от большего внизу к меньшему наверху. Игра заключается в том, чтобы передвинуть диски с одного стержня на другой, не нарушая следующие правила:

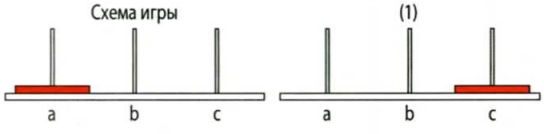
— За один ход может быть передвинут только один диск;

— Нельзя перемещать диск на соседний стержень, если на него нанизан диск меньшего размера.

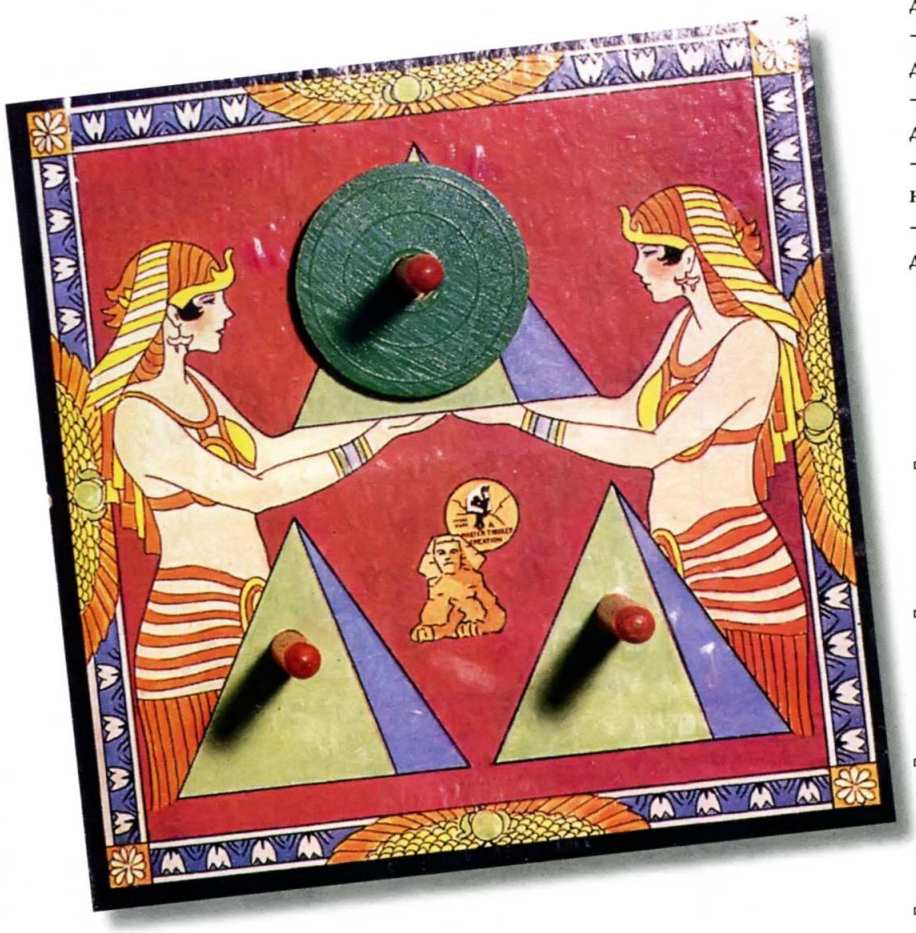
Когда дисков совсем немного, игра кажется легкой. Но с увеличением количества дисков растет и количество шагов, которые надо предпринять, чтобы диски перенести, а вместе с этим усложняется и сама игра.

Во сколько шагов решается головоломка?

В случае с одним диском ответ ясен — переместить его на любой из стержней можно одним движением:



▼ *Необычного вида доска для игры на рисунке внизу, на самом деле, не что иное, как Ханойская башня, но оформленная в египетском вкусе.*



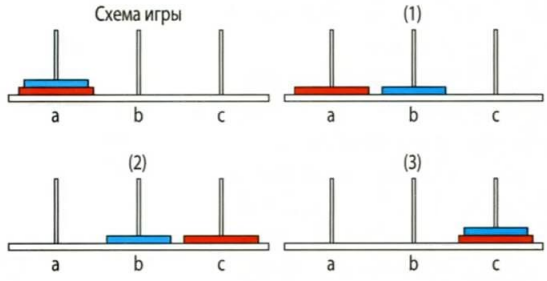
В случае с двумя дисками решение включает в себя несколько действий:

— Сначала перемещаем маленький диск на стержень B;

— Потом перемещаем большой диск на стержень C;

— И третьим движением перемещаем маленький диск на стержень C.

Всего три шага.



В случае с тремя дисками количество шагов увеличится:

— Первым движением перемещаем маленький диск на стержень C;

— Вторым движением перемещаем средний диск на стержень B;

— Третьим движением перемещаем маленький диск на стержень B;

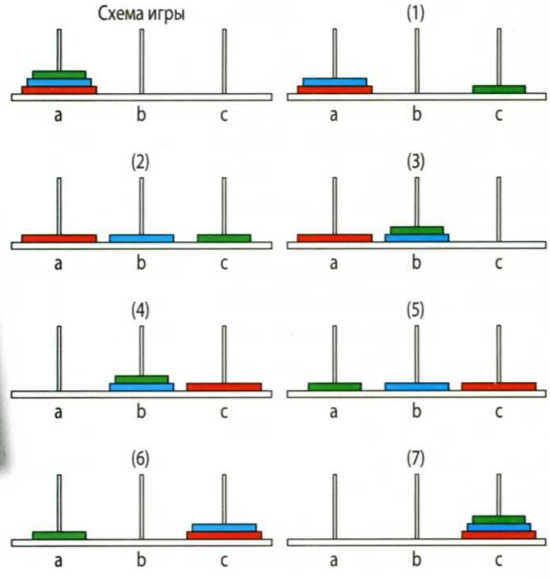
— Четвертым движением перемещаем большой диск на стержень C;

— Пятым движением перемещаем маленький диск на стержень A;

— Шестым движением перемещаем средний диск на стержень C;

— И седьмым движением переносим маленький диск на стержень C.

Итак, семь шагов:



Как становится видно, процесс делится на три части. Сначала переносится башня из двух дисков со стержня A на стержень B. Затем перемещается большой диск со стержня A на стержень C, и в итоге, также стараясь максимально сократить количество шагов, со стержня B на стержень C переносится башенка из двух дисков. Первая и третья фазы возможны потому, что там не присутствует большой диск: словно его и нет на стержне. Таким образом, если для того, чтобы передвинуть башню из двух дисков, нам необходимо было как минимум 3 шага, то для перемещения башни из трех дисков будет необходимо как минимум 3 + + 1 + 3 = 7 шагов.

Аналогичным образом решается и Ханойская башня из четырех дисков. Сначала три верхних перемещаются на стержень B, затем большой диск — с A на C, и в конце оставшиеся три диска со стержня B на C. Здесь уже необходимо как минимум 7 + 1 + 7 = 15 шагов.

Образец решения формируется сам. Таблица, приведенная ниже, показывает минимальное количество шагов, которое необходимо выполнить, чтобы решить головоломку с любым количеством дисков.

Кол-во дисков	Минимальное кол-во шагов
1	$1 = 2^1 - 1$
2	$1 + 1 + 1 = 2^2 - 1$
3	$3 + 1 + 3 = 2^3 - 1$
4	$7 + 1 + 7 = 2^4 - 1$
...	...
8	$127 + 1 + 127 = 2^8 - 1$
...	...

И так по нарастающей. Для десяти дисков необходимо как минимум $2^{10} - 1 = 1023$ шага, а для шестидесяти четырех — $264 - 1 =$ = 18 446 744 073 709 551 615 шагов.

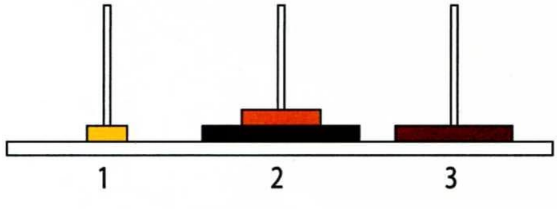
Фрактальная башня

Существует удивительная взаимосвязь между Ханойской башней и любопытным фракталом, названным треугольником Серпинского. Эта взаимосвязь была описана в 1992 году Яном Стюартом, и с момента построения графа ее тяжело не заметить. Следуя ходу мысли Стюарта, можно увидеть, что в случае с Ханойской башней каждая из конфигураций присоединяет к себе кроме точки еще и упорядоченный ряд чисел, равный количеству дисков. Выглядит это следующим образом:

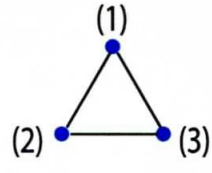
— Сначала пронумеровываются стержни с 1 по 3. Например, левый стержень получает номер 1, средний — 2, правый — 3;

— Затем к каждой конфигурации присоединяется ряд чисел: первый представляет номер стержня, который занимает самый маленький диск. Второй — номер стержня, занятого диском следующего размера, и так далее.

Так, например, ряд (1, 2, 3, 2) представляет следующую конфигурацию четырех дисков:



Предполагается, что на одном стержне диски упорядочены по размеру от большего к меньшему, как этого требуют правила игры. Таким образом, каждый ряд чисел определяет единственную возможную конфигурацию.

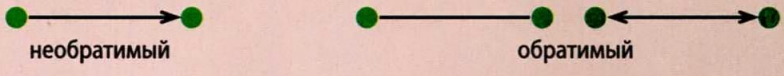


Как видно по вышеприведенному графу, для Ханойской башни с одним диском единственно возможна следующая конфигурация: (1), (2), (3).

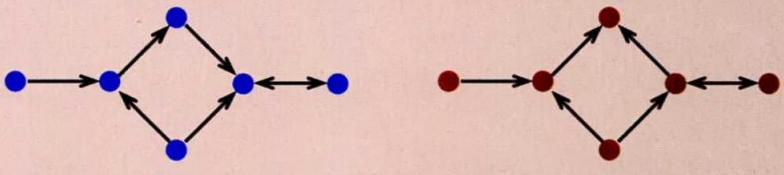
Игры и графы

Граф — это совокупность точек, объединенных линиями. Такие линии называются дугами. Точки представляются как объекты (люди, числа, структуры), а дуги представляются как связь между этими точками. В математике существует целый раздел, посвященный их изучению,— теория графов. В мире игр-головоломок многие задачки можно отнести к графам, и как следствие, применить для их решения инструменты, присущие этому разделу науки.

Чтобы построить граф к игре, надо соотнести одну точку с каждой возможной позицией. Затем, если ход разрешен правилами игры, две точки соединяются стрелкой. Если движение необратимо, то стрелка будет направлена в одну сторону, если обратимо, то стрелка будет двойной и соединит обе точки.



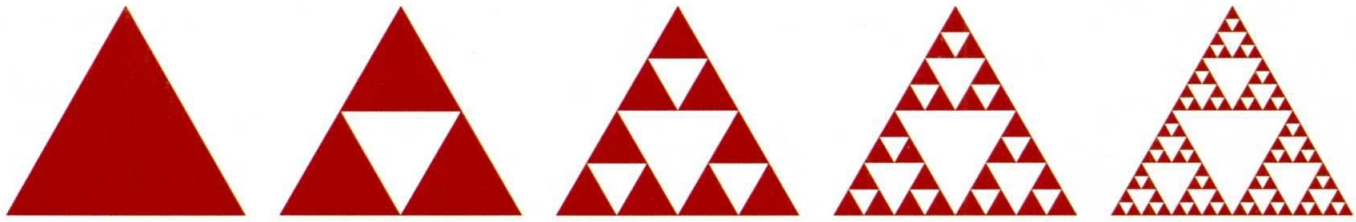
Ключ к разгадке паззла состоит в том, чтобы найти путь от начальной точки к конечной. Если его не существует, то головоломка не имеет решения. Например:



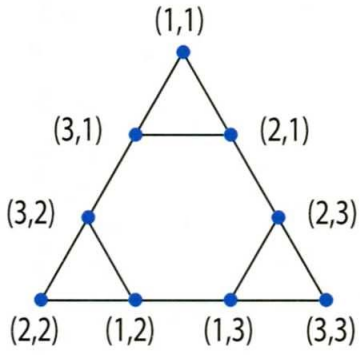
Фрактальный треугольник

Это треугольник Серпинского — геометрический объект из рода фракталов. Как многие фракталы, он получился благодаря бесконечным повторениям одного и того же элемента.

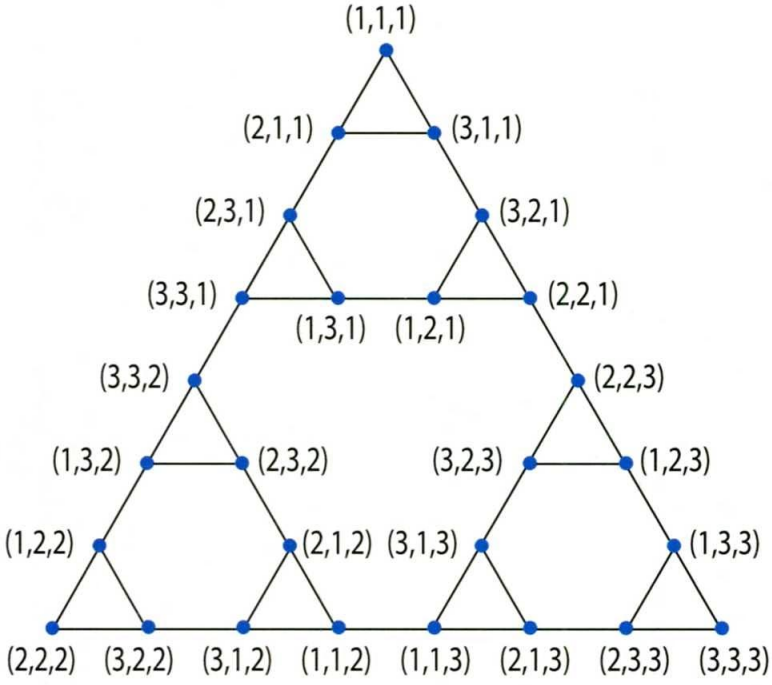
В данном случае — образования треугольников меньшего размера. Треугольник Серпинского — это результат многократного изображения меньших треугольников внутри большего.



Для Ханойской башни из двух дисков есть девять возможных конфигураций, связанных между собой так, как показывает граф:



По аналогии, для трех дисков существует 27 различных конфигураций, как показано ниже:



Рисуя дуги графа Ханойской башни, со временем замечаешь, что они начинают напоминать треугольник Серпинского. По мере увеличения количества дисков совпадения между двумя рисунками становятся все более явными.

Двоичная система счисления

Решение Ханойской башни теснейшим образом связано с системой двоичного счисления. Последовательно нумеруя диски 1, 2, 3, 4 и так далее от меньшего к большему, каждый шаг в игре можно представить одним номером, номером играющего диска. Таким образом, семь шагов при игре с тремя дисками можно представить в виде следующих номеров: 1, 2, 1, 3, 1, 2, 1 (см. стр.2).

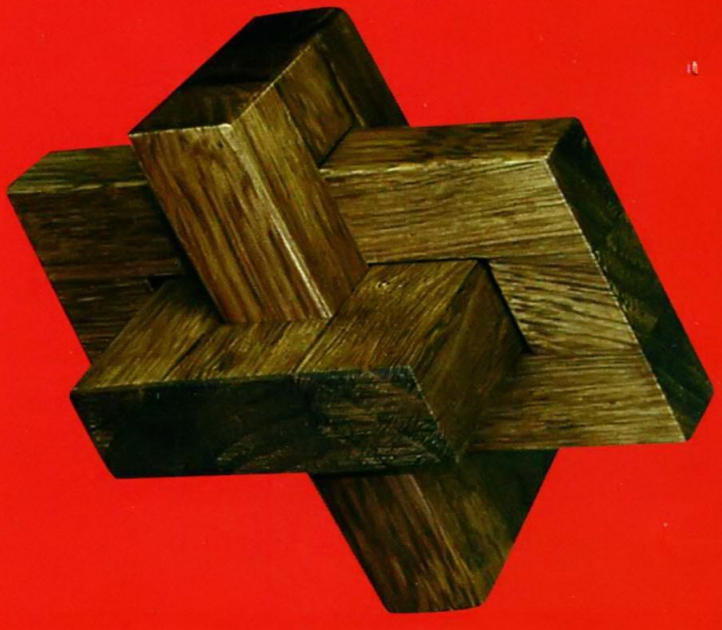
Затем пишутся двоичные числа в возрастающем порядке, и становится видно, что между двоичным числом и следующим за ним всегда есть еще одно от 0 до 1 в любой из трех позиций.

Число по десятичной шкале	Число по бинарной шкале	Позиция, которую занимает число от 0 до 1
0	000	
1	001	1
2	010	2
3	011	1
4	100	3
5	101	1
6	110	2
7	111	1

Глядя на положение цифр с правой стороны, можно увидеть удивительную последовательность ходов в игре Ханойская башня. И эта связь с двоичной системой работает вне зависимости от количества дисков в игре.

В следующем выпуске через 2 недели

Косой узел



Математические обозначения

Цифробуквенный «винегрет»

Отец алгебры

Франсуа Виет

Вычислители

Люди-калькуляторы

Лучшее из Генри Дьюдени

Загадки о времени и скорости

Спрашивайте в киосках!